Kali Linux

Official

Documentation

目錄

Kali Linux 中文文档

译者：huatux

来源：Kali Linux Official Documentation

00. Kali Linux介绍

Kali Linux默认密码

Linux root的默认密码是toor

默认的root密码

安装Kali期间可以给*root*用户设置一个密码.但如果你用的是live、i386、amd64、VMware或ARM镜像时,root的默认密码是**toor**.

01. 下载Kali Linux

封装定制的Kali Live ISO

打造专属的Kali ISO – 简介

封装定制的Kali ISO很简单,很有趣,很有意义.你可以用Debian的live-build脚本对Kali ISO进行全面的配置.这些脚本以一系列配置文件的方式对镜像进行全面的自动定制,让任何人都可以轻易地就能打造一个Live系统镜像.官方发布的Kali ISO也采用了这些脚本.

前提

最理想的是在预装Kali的环境里定制你的Kali ISO.如果不是这样,请务必使用最新版本的live-build脚本(3.x分支的脚本可用于Debian wheezy).

准备开始

首先我们要用以下命令搭建好定制Kali ISO的环境:

```
apt-get install git live-build cdebootstrap kali-archive-keyring
git clone git://git.kali.org/live-build-config.git
cd live-build-config
lb config
```

封装Kali ISO的配置(可选)

config目录里包含了定制ISO的各种重要的自定义选项,这些选项在Debian的live build 3.x页面有文档说明.然而如果你没有耐心,请特别注意以下的配置文件:

config/package-lists/kali.list.chroot – 包含要安装在Kali ISO里的软件包的列表.你可以指定移除已经安装的软件包.也可以切换你的Kali ISO的桌面环境(KDE,Gnome,XFCE,LXDE等).

hooks/ – hooks 目录允许我们在不同阶段调用脚本封装定制Kali Live ISO.更多关于hooks的信息,参考live build 手册.举个例子,Kali是这样添加取证模式的引导菜单的:

```
$ cat config/hooks/forensic-menu.binary
#!/bin/sh

cat >>binary/isolinux/live.cfg <<END

label live-forensic
    menu label ^Live (forensic mode)
    linux /live/vmlinuz
    initrd /live/initrd.img
    append boot=live noconfig username=root hostname=kali noswap noautomount
END
```

封装ISO

在封装ISO之前,可以指定需要的架构,选择amd64或者i386.还要注意"lb build"需要root权限.如果你不指定架构,live build将根据你现在使用的架构来封装ISO.

如果你想在在32位系统封装64位的ISO,务必打开多架构支持:

```
dpkg --add-architecture amd64
apt-get update
```

配置live-build封装64位或者32位ISO:

```
lb config --architecture amd64 # for 64 bit
# ...or...
lb config --architecture i386  # for 32 bit

lb build
```

最后一个命令需要一些时间,因为它下载所有需要的软件包然后封装ISO.可以先去喝杯咖啡.

为今后封装ISO提速

如果你打算经常定制ISO,你可以把kali的软件包缓存在本地便于今后的封装.最简单的就是安装**apt-cacher-ng**,然后在每次打包时配置http_proxy环境变量.

```
apt-get install apt-cacher-ng
/etc/init.d/apt-cacher-ng start
export http_proxy=http://localhost:3142/
.... # setup and configure your live build
lb config --apt-http-proxy http://127.0.0.1:3142/
lb build
```

用Live U盘安装Kali Linux

从U盘启动然后安装Kali是我们最喜欢并且是运行Kali最快(容易)的方法.为此,我们首先要把Kali的ISO克隆到U盘.如果你经常使用Kali Linux U盘,请在克隆前阅读完整的文档.

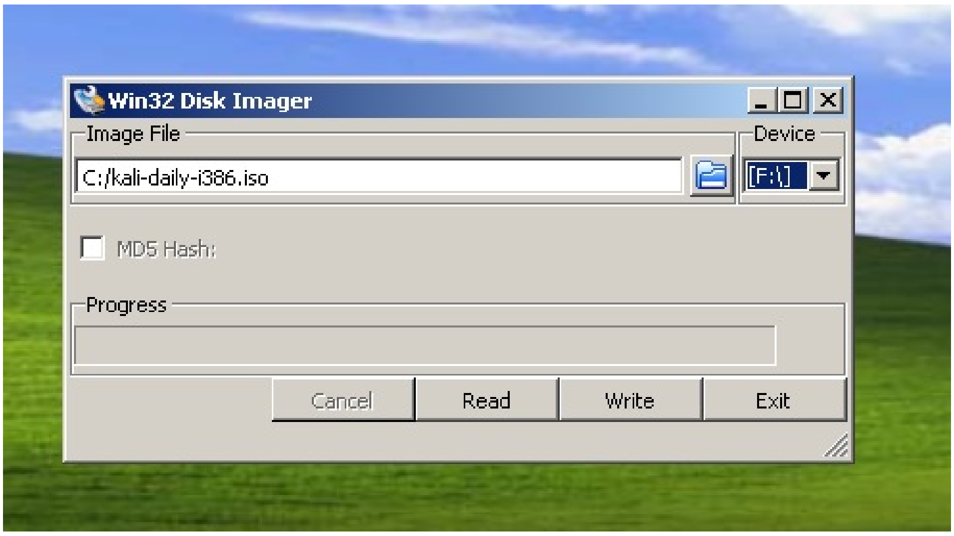
准备USB镜象

1. 下载Kali linux.
2. 如果你用的是Windows,下载Win32 Disk Imager.
3. *nix类系统不需要额外的软件.
4. 一块U盘(至少 2GB 容量).

Kali Linux Live U盘安装过程

在用Windows的电脑上克隆Kali

1. 插入U盘.运行Win32 Disk Imager.
2. 选择Kali Linux ISO文件作为被克隆的文件,然后核实要克隆的U盘是否正确.



1. 克隆完成后,从Windows机器安全弹出U盘.现在你可以用U盘启动Kali Linux了.

在用Linux的电脑上克隆Kali

在Linux环境下制作可启动的Kali Linux U盘很容易.下载好Kali ISO文件后,你可以用dd把它克隆到U盘:

警告！虽然在U盘上克隆Kali过程很简单,但是如果你不懂你正在用dd做什么,很容易破坏引导分区.

1. 插入U盘.
2. 用**dmesg**确认你的U盘设备块名.
3. 开始克隆Kali ISO文件到U盘(谨慎操作！):

    ```
    dd if=kali.iso of=/dev/sdb bs=512k
    ```

就这样!你现在可以用U盘启动到Kali Live/Installer环境了.

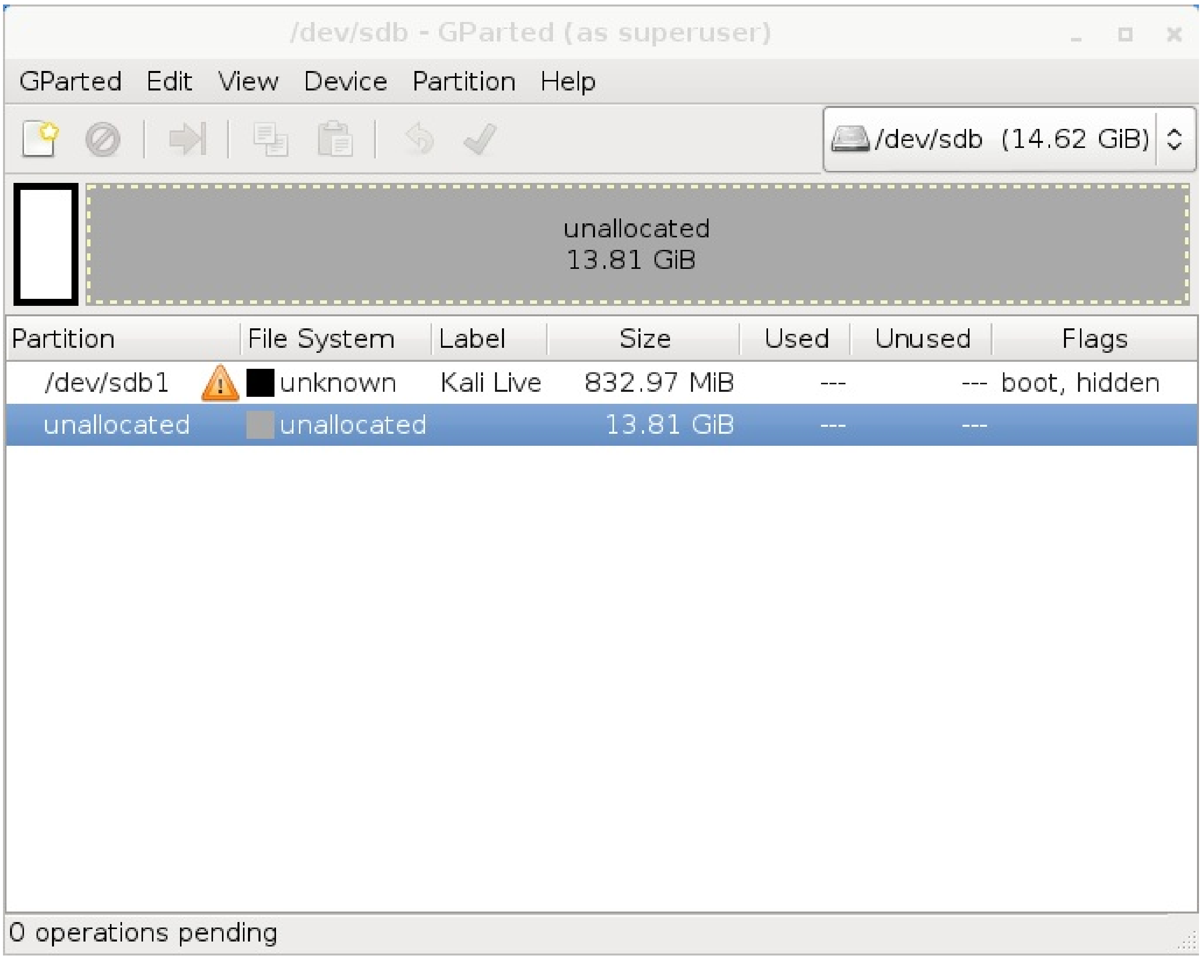
为你的U盘添加Persistence功能

在某些情况下.为你的Kali Linux镜象添加persistence功能(在Live启动的时候可以保存和修改文件)非常有用.为了给你的Kali Linux U盘启动persistent功能,按照以下步骤.本例中,我们假设我们的设备块名是**/dev/sdb**.如果你想添加persistence功能,需要一块比上面提到的要求更大容量的U盘.

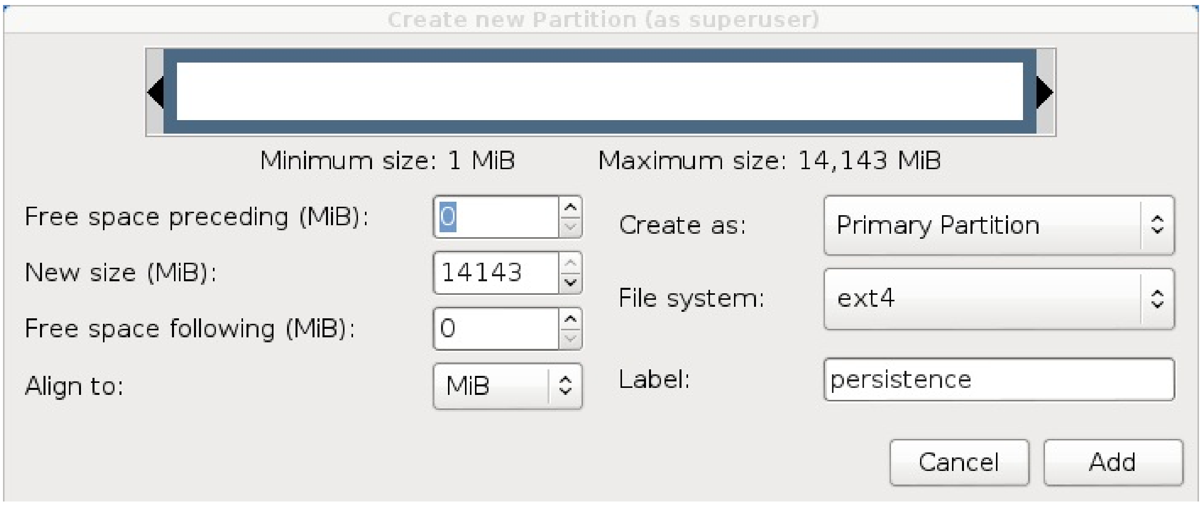
1. 克隆Kali Linux ISO到U盘和上面讲解的一样,用dd在"用Linux的电脑上克隆Kali".
2. 在U盘创建并格式化额外的分区.本例中我们用**gparted**

    ```
    gparted /dev/sdb
    ```

3. 现在你的分区方案应该和下图类似:



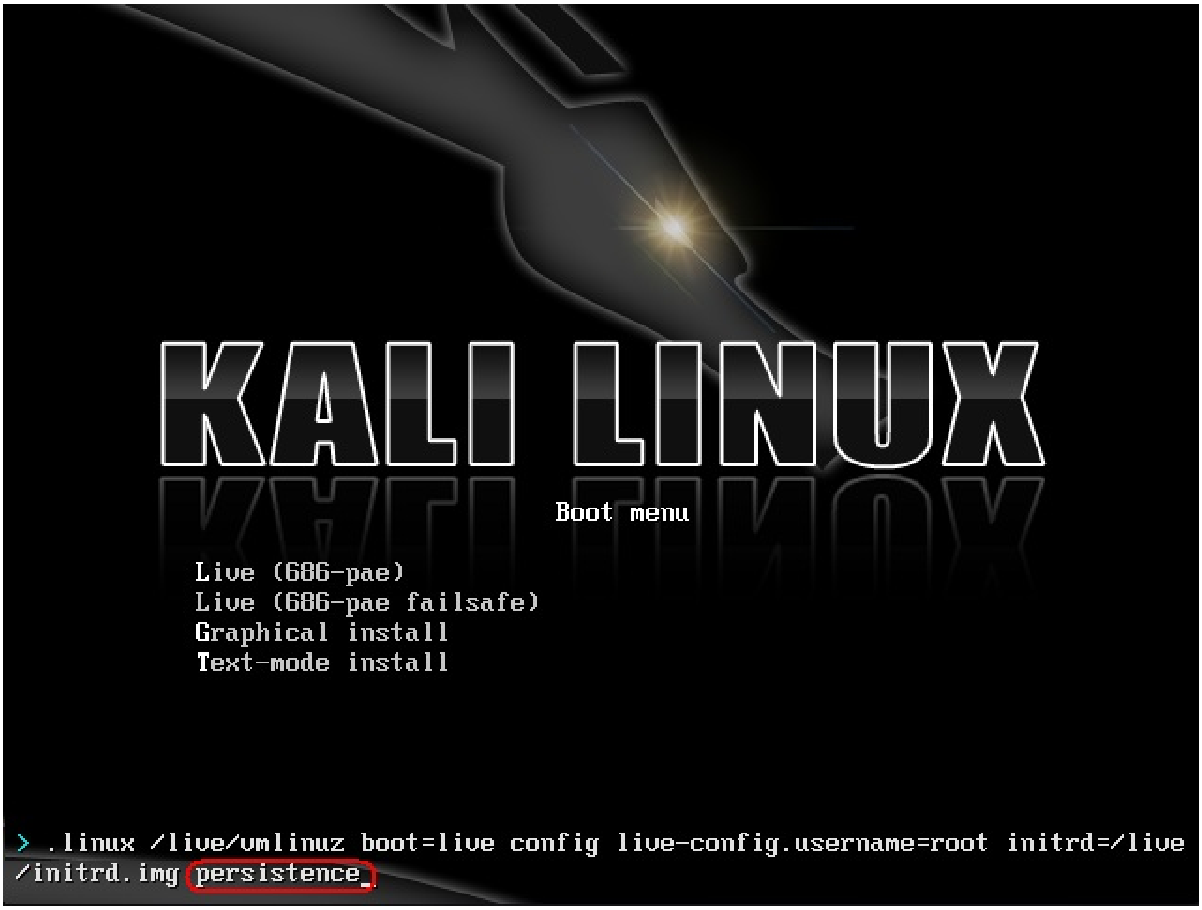
4. 着手于格式化一个你要用于persistence功能的理想大小的新分区.在此例,我们使用所有剩余可用空间.确保新创建的分区卷名是*persistence*然后格式化成*ext4*文件系统.



5. 这步完成后,用以下命令挂载用于persistence功能的U盘分区:

```
mkdir /mnt/usb
mount /dev/sdb2 /mnt/usb
echo "/ union" &gt;&gt; /mnt/usb/persistence.conf
umount /mnt/usb
```

6. 插入U盘到你要启动的电脑.务必设置BIOS从USB设备启动.当显示Kali Linux启动画面时,从菜单选择“Live boot”(不要按下回车),然后按下Tab键.这将允许你编辑启动参数,在每次你想挂载你的persistent 存储时添加“persistence”到boot参数行的最后.



02. 制作定制的Kali镜像

03. 安装Kali Linux

无线驱动疑难排解

如果你不确定你在找什么,那么Linux的无线驱动问题的疑难排解将会是个挫折.本文将以一般指引的方式来帮助你更好的找到解决无线问题所需要的信息.

仔细的阅读错误信息,经常能告诉你怎么回事和如何解决.或者,使用Google.

1. 没有网卡

- 愚蠢的问题:它是无线网卡吗?(我们见过很多次了)
- 无线网卡插好了吗?
- **lsusb**或者**lspci**能看到它吗(手机除外)?可能需要更新pci ids和usb ids
- **dmesg**里有关于加载驱动或加载失败的信息吗
- 是Kali的虚拟机吗?如果是,除非你的是USB网卡,否则不可用(VMWare/VirtualBox/QEMU会虚拟每个PCI硬件).USB网卡连到虚拟机了吗?
- 如果dmesg里没有信息并且不是虚拟机,那么你可能需要试试最新的*Compat-wireless*(有时需要固件)->检查linux无线驱动

2. 有网卡但不能做任何事

- 看错误信息
- 如果没有错误信息,就执行**dmesg|tail**,可能会告诉你怎么回事
- 可能缺少固件
- 检查rfkill和硬件开关还有BIOS选项

3. 没有监听模式

- STA驱动(Ralink, Broadcom)还有其他厂商生产提供的驱动都不支持监听模式
- ndiswrapper 不支持监听模式.永远不会.
- Airodump-ng/Wireshark 不显示任何信息:检查rfkill和硬件开关还有BIOS选项

4. 注入

- 用aireplay-ng -9测试(用airmon-ng确定网卡处于监听模式)
- Airmon-ng不显示芯片信息:这不是大问题,只是不能获取网卡的信息,不会影响网卡的功能.
- 处于监听模式但不能注入:检查rfkill和硬件开关还有BIOS选项
- 网络管理器有时和Aircrack工具包有冲突.运行**airmon-ng check kill**来杀掉这些进程.

附加链接

- Will my card work with Aircrack-ng?
- Compat-wireless

用Mini ISO通过网络安装Kali Linux

用Mini ISO安装Kali Linux

用Kali mini ISO可以方便地"从头"开始安装一个最小化的Linux.Mini ISO会从我们的源下载所需的软件包,这意味着要使用这种安装方式你需要一个快速的网络.

安装条件

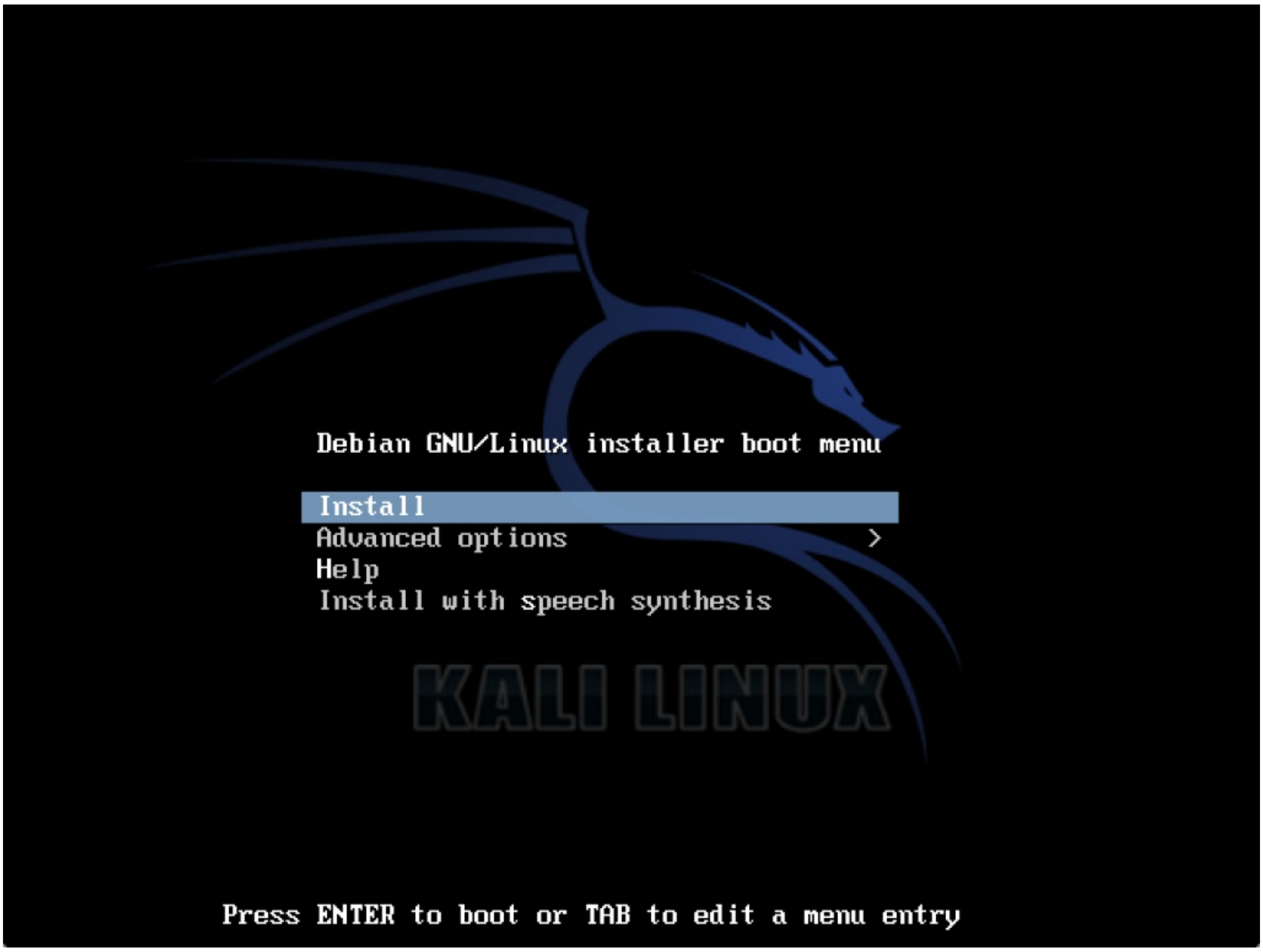
- 安装Kali Linux最少8G硬盘可用空间.
- i386和amd64架构,最低512MB内存.
- CD-DVD光驱/支持USB引导

准备安装

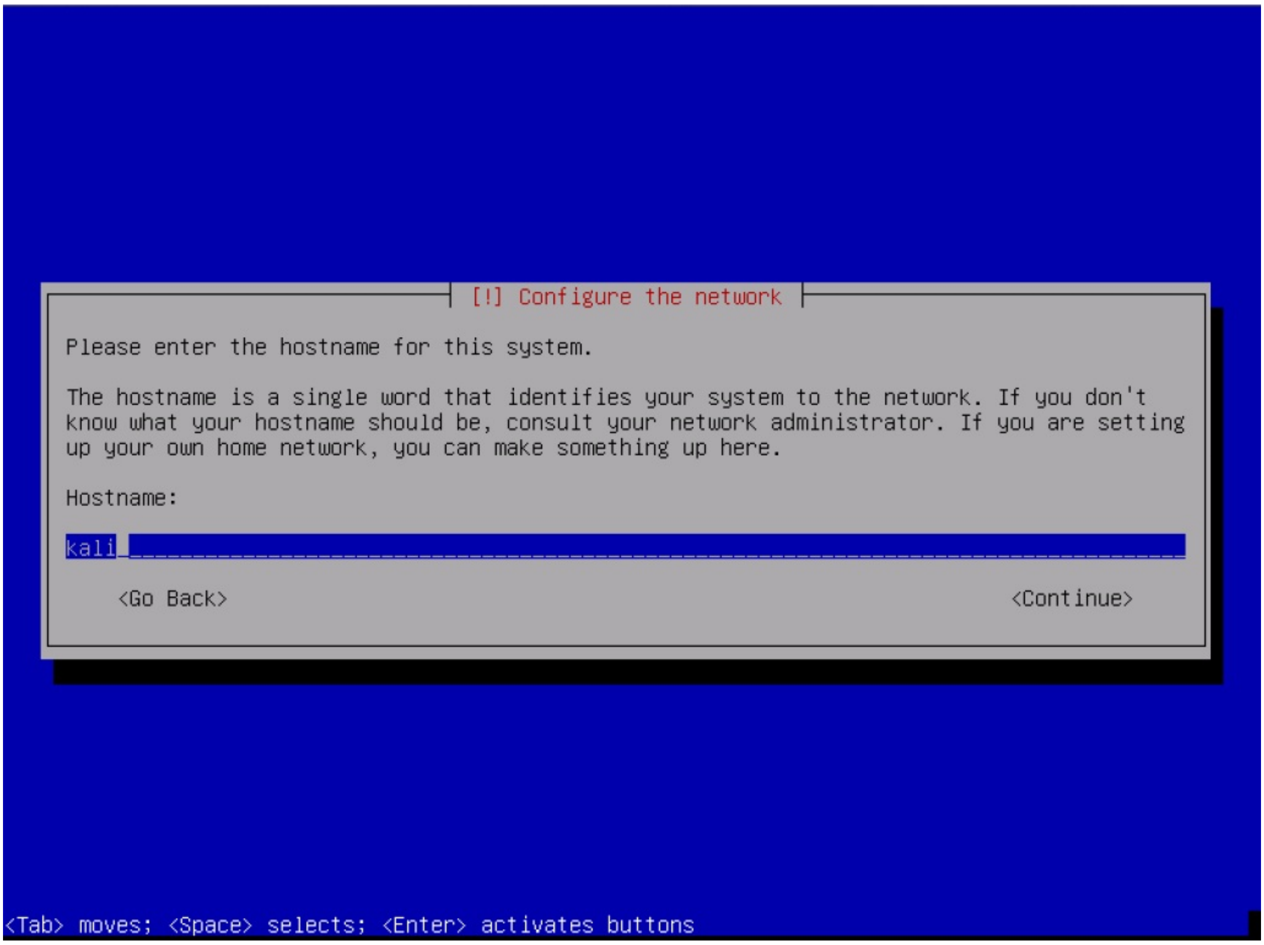
1. 下载Kali mini ISO.
2. 把Kali Linux刻录到DVD盘或制作Kali Linux镜像U盘.
3. 确认你电脑的BIOS设置了从CD/USB引导.

Kali Linux安装步骤

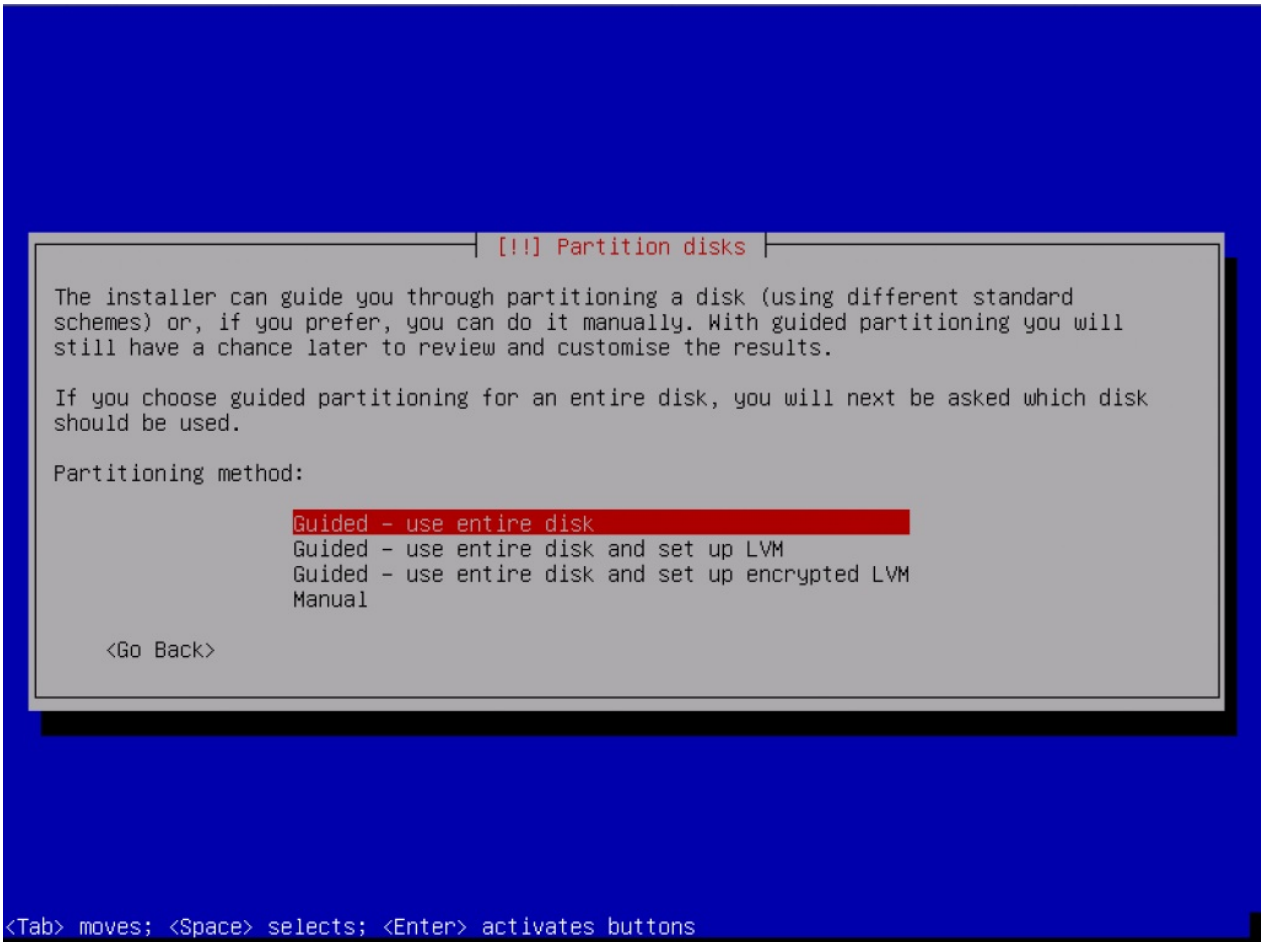
当你用mini ISO启动时,会出现一个有很多选项的启动界面,本文中,我们将进行简单的基本安装.



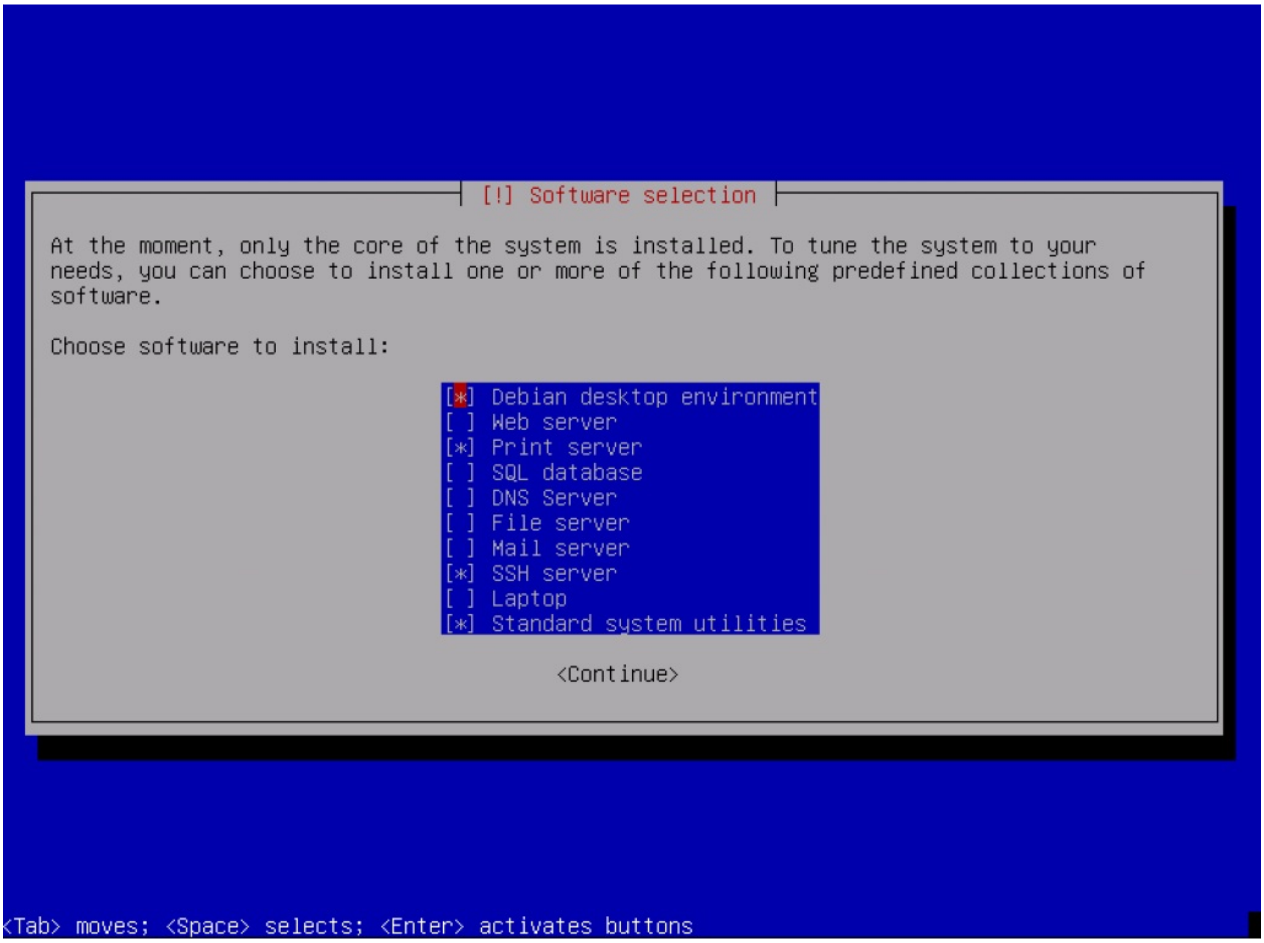
接下来会提示你各种设置,例如语言和键盘布局,然后你要为系统设置一个主机名称,在这里我们用了默认的*kali*.



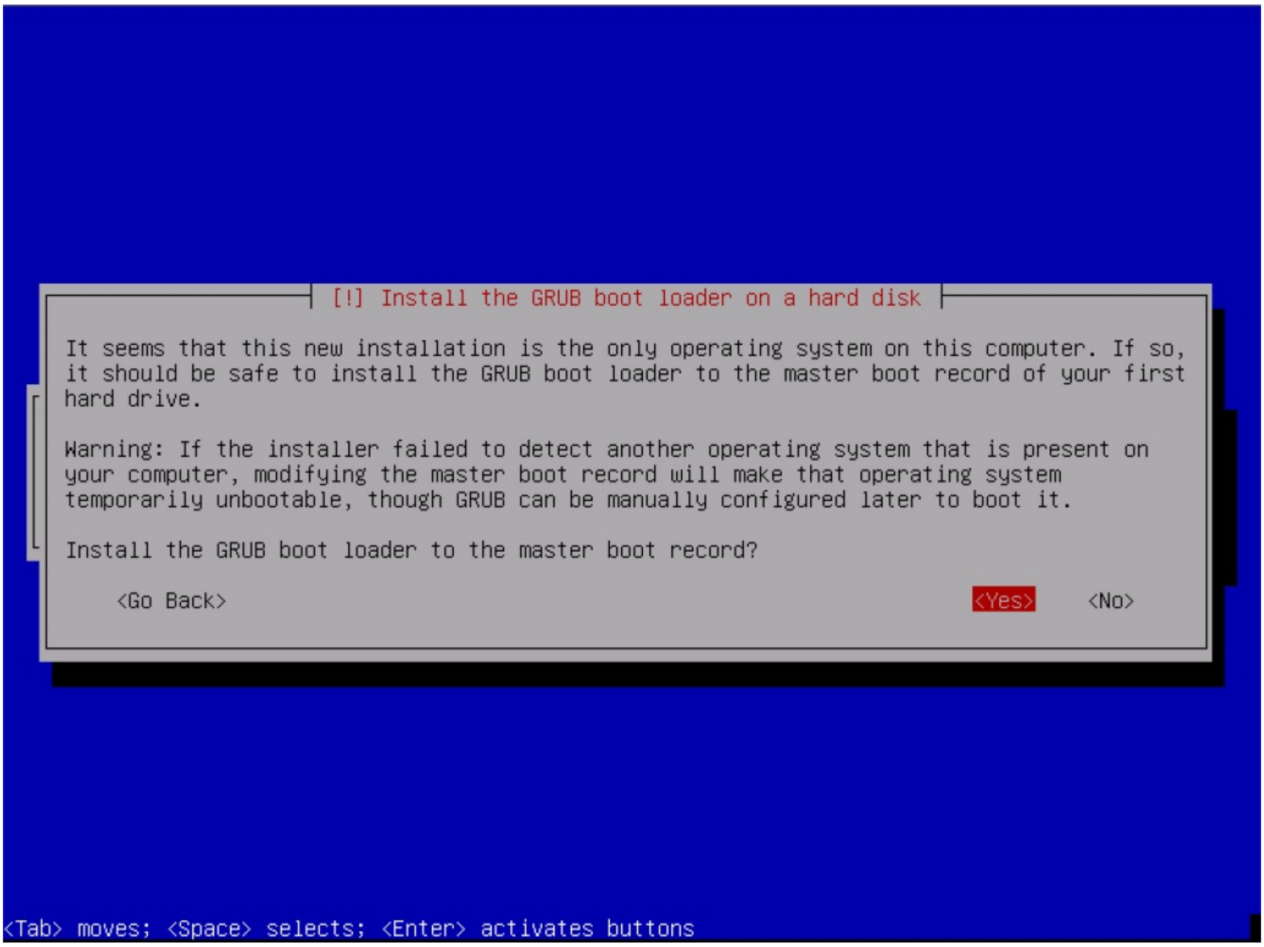
接下来选择时区,然后会出现分区选项,为了快速起见,本文我们选'Guided – use entire disk'这个选项,一直按照提示做,直到创建新的分区格局.



为了减少网络流量,默认只选择了一小部分的软件包.如果你要添加另外的服务或功能,可以在这个界面做选择.



至此,安装程序会在系统上下载并安装它所需的软件包.这步花的时间与你的网速有关.最后,会提示你安装GRUB以完成整个安装过程.



安装后

现在你已经完成了Kali Linux的安装,是时候定制你的系统了.官方网站上的Kali常见问题里有更多信息,你也可以在我们的用户论坛找到更多的技巧.

通过网络PXE安装Kali Linux

搭建PXE服务器

通过网络(PXE)来启动和安装Kali,对于一台没有光驱或者USB端口的笔记本很有用,甚至对一个企业部署预安装Kali都很有用.

首先,我们要安装*dnsmasq*以提供 DHCP/TFTP 服务,然后编辑*dnsmasq.conf*这个配置文件.

```
apt-get install dnsmasq
nano /etc/dnsmasq.conf
```

在*dnsmasq.conf*文件中,按如下所示启用DHCP,TFTP和PXE启动,根据你的环境修改*dhcp-range*:

```
interface=eth0
dhcp-range=192.168.8.100,192.168.8.254,12h
dhcp-boot=pxelinux.0
enable-tftp
tftp-root=/tftpboot/
```

编辑好了之后我们需要重启dnsmasq服务使之生效.

```
service dnsmasq restart
```

下载安装kali PXE网络启动镜像

现在,我们要创建一个文件夹用于存放Kali网络启动镜像,还有我们欲从Kali软件源下载的镜像.

```
mkdir -p /tftpboot
cd /tftpboot
# for 64 bit systems:
wget http://repo.kali.org/kali/dists/kali/main/installer-amd64/current/images/netboot/net
# for 32 bit systems:
wget http://repo.kali.org/kali/dists/kali/main/installer-i386/current/images/netboot/netb
tar zxpf netboot.tar.gz
rm netboot.tar.gz
```

设置要安装Kali的机器从网络启动

都配置好之后,现在你可以启动你的电脑.,然后配置它从网络启动.它会从PXE服务器获取到IP地址然后启动kali.

加密安装Kali Linux

有时我们希望采用全盘加密的方式来加密我们的敏感信息.你可以使用Kali安装程序把它安装到硬盘或是U盘的加密LVM逻辑卷.安装过程除了加密LVM逻辑卷部分以外,与"常规的Kali Linux安装"非常类似.

加密安装Kali Linux条件

安装Kali Linux到你的电脑过程很简单.首先你需要兼容的电脑硬件.最低硬件要求如下,更好的硬件性能会更好.i386镜象默认使用PAE内核,所以你能在大于4GB内存的机器运行它.下载Kali Linux然后刻录DVD盘,或准备好一块Kali Linux Live U盘作为安装媒介.

安装条件

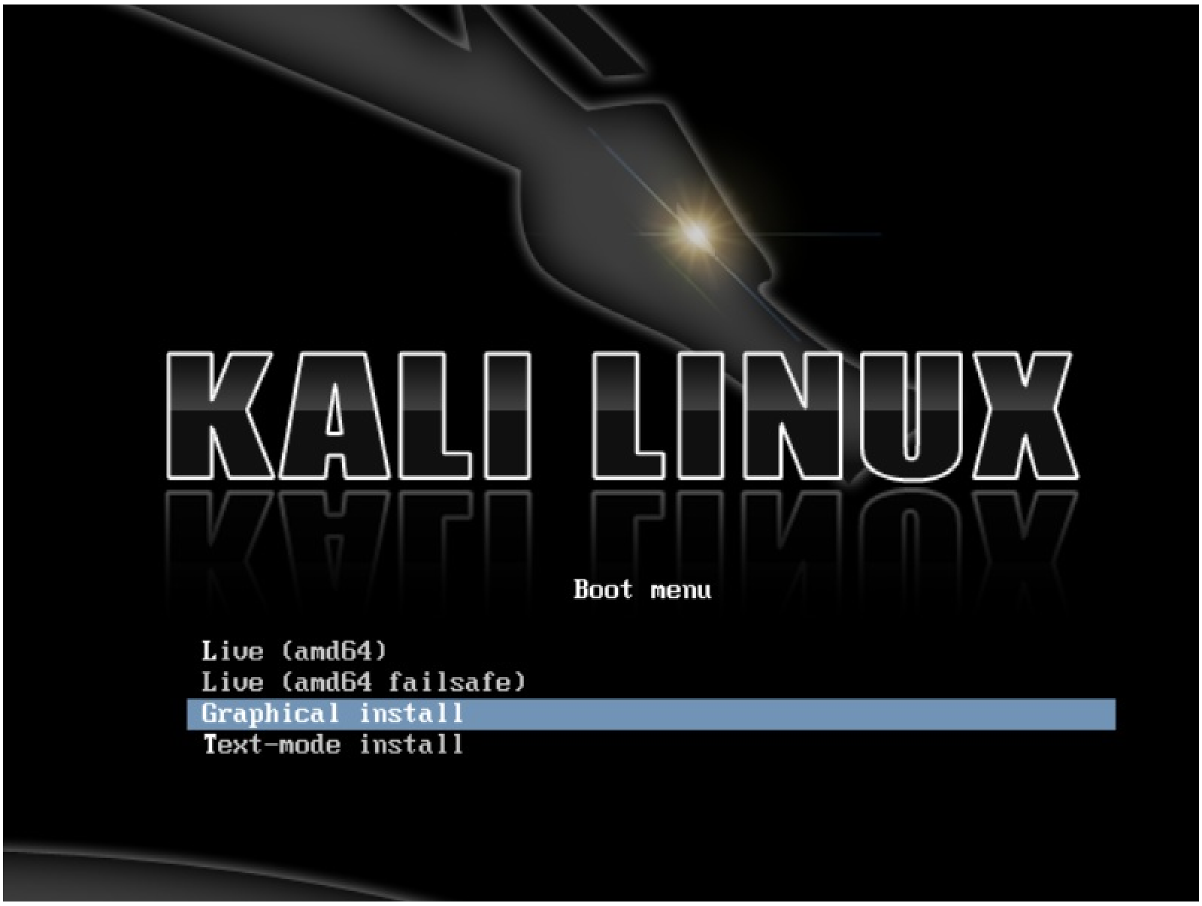
- 安装Kali Linux需要最少8G硬盘可用空间.
- i386和amd64架构,最低512MB内存.
- CD-DVD光驱/支持USB引导

准备安装

1. 下载Kali Linux.
2. 把Kali Linux刻录到DVD盘或制作Kali Linux镜像U盘.
3. 确认你电脑的BIOS设置了从CD/USB引导.

Kali Linux安装步骤

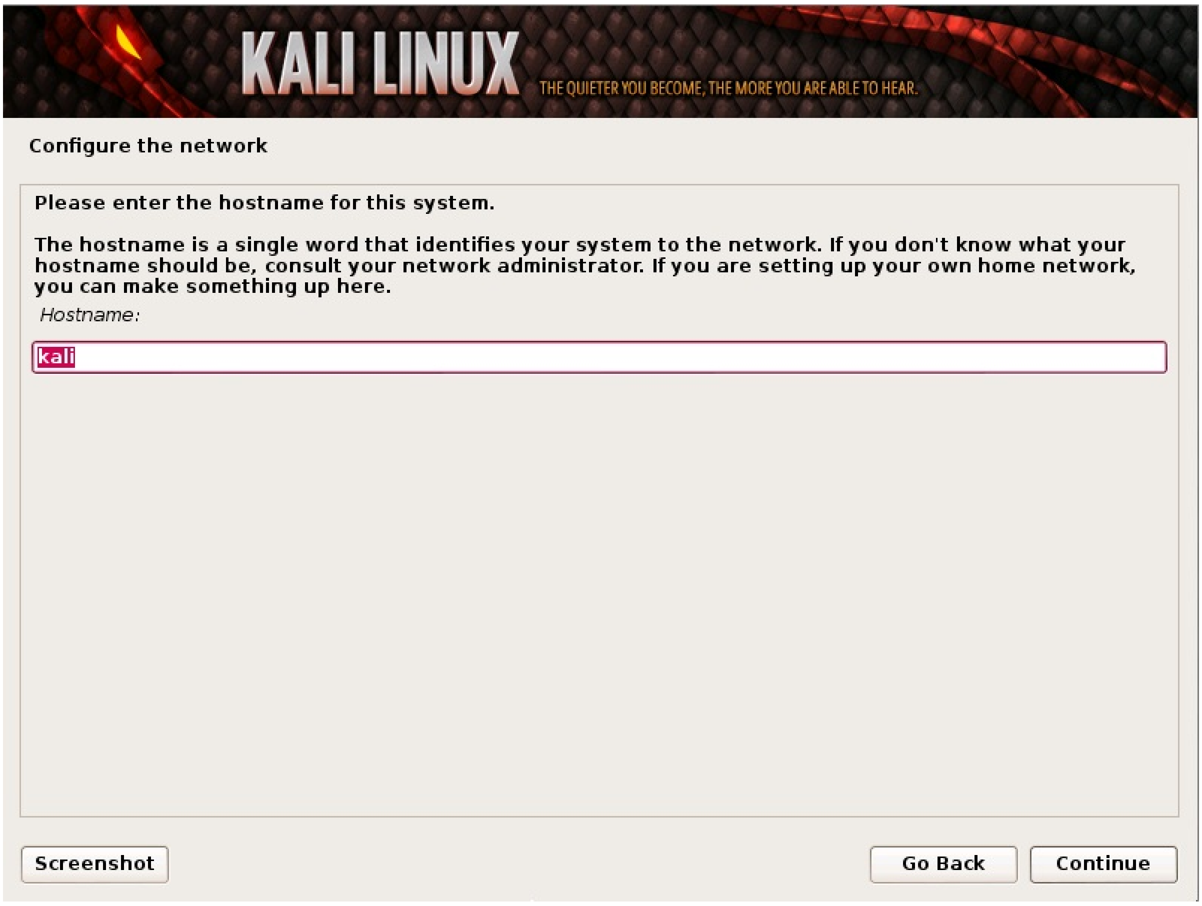
1. 开始安装,从你选择的安装媒介启动. 你会看到Kali的引导界面.选择图形界面或文本模式安装.此处,我们选择图形界面安装.



2. 选择你的首选语言和国家.你会被提示为你的键盘配置适当的Keymap.



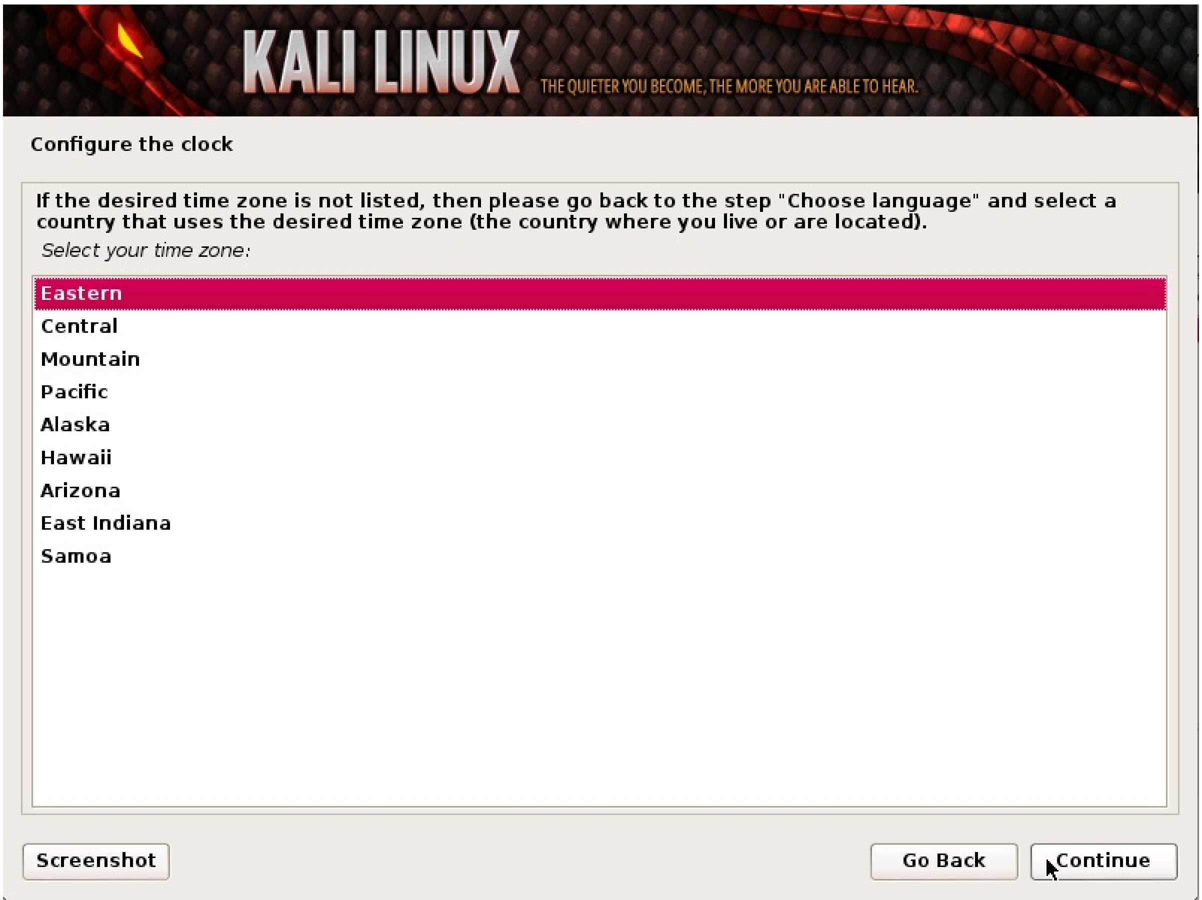
3. 安装器会复制镜象到你的硬盘,探测你的网络接口,然后提示你为你的系统输入主机名.此例,我们输入"Kali"作为主机名.



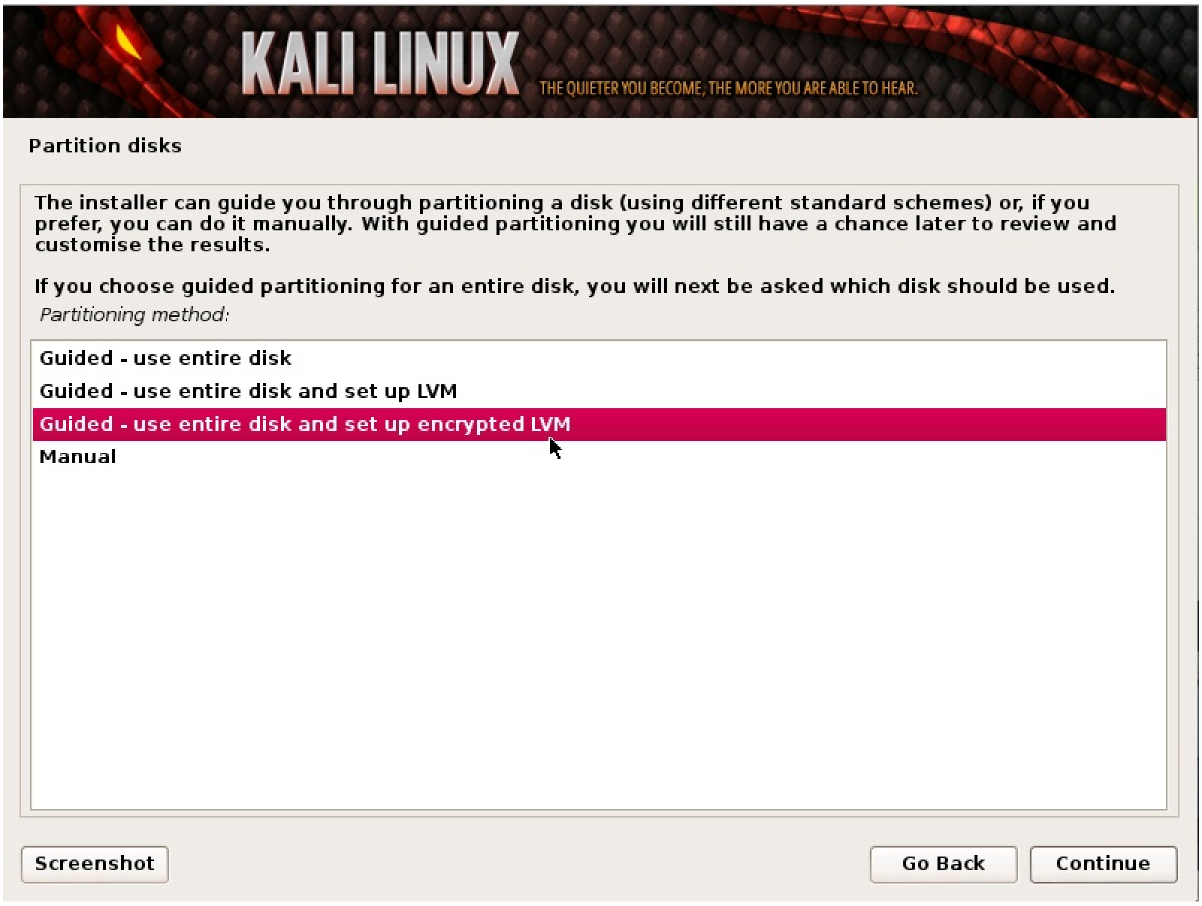
4. 为root账户输入一个强健的密码


KALI LINUX
THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.
Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
Please enter the same root password again to verify that you have typed it correctly.
Re-enter password to verify:
Screenshot
Go Back
Continue

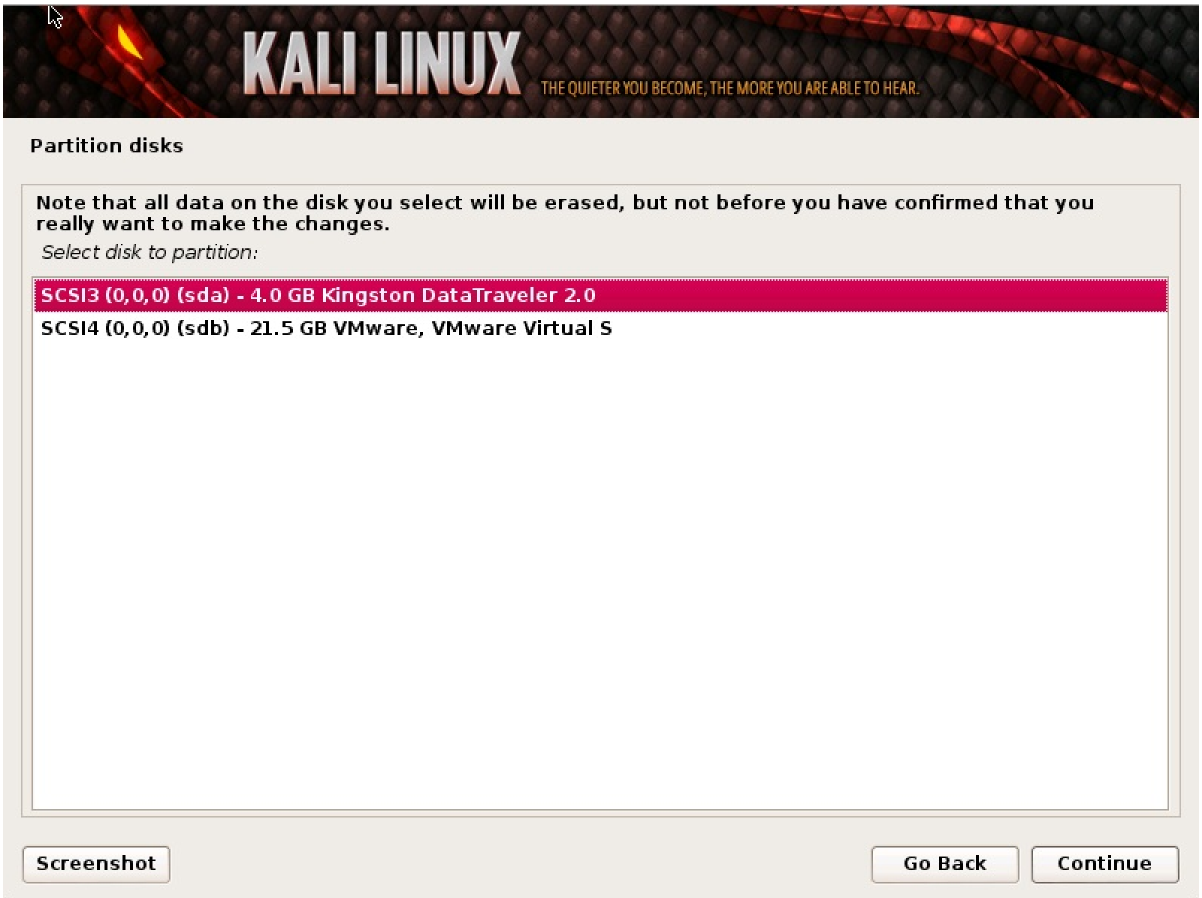
5. 下一步设置时区.


KALI LINUX
THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.
Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
Screenshot
Go Back
Continue

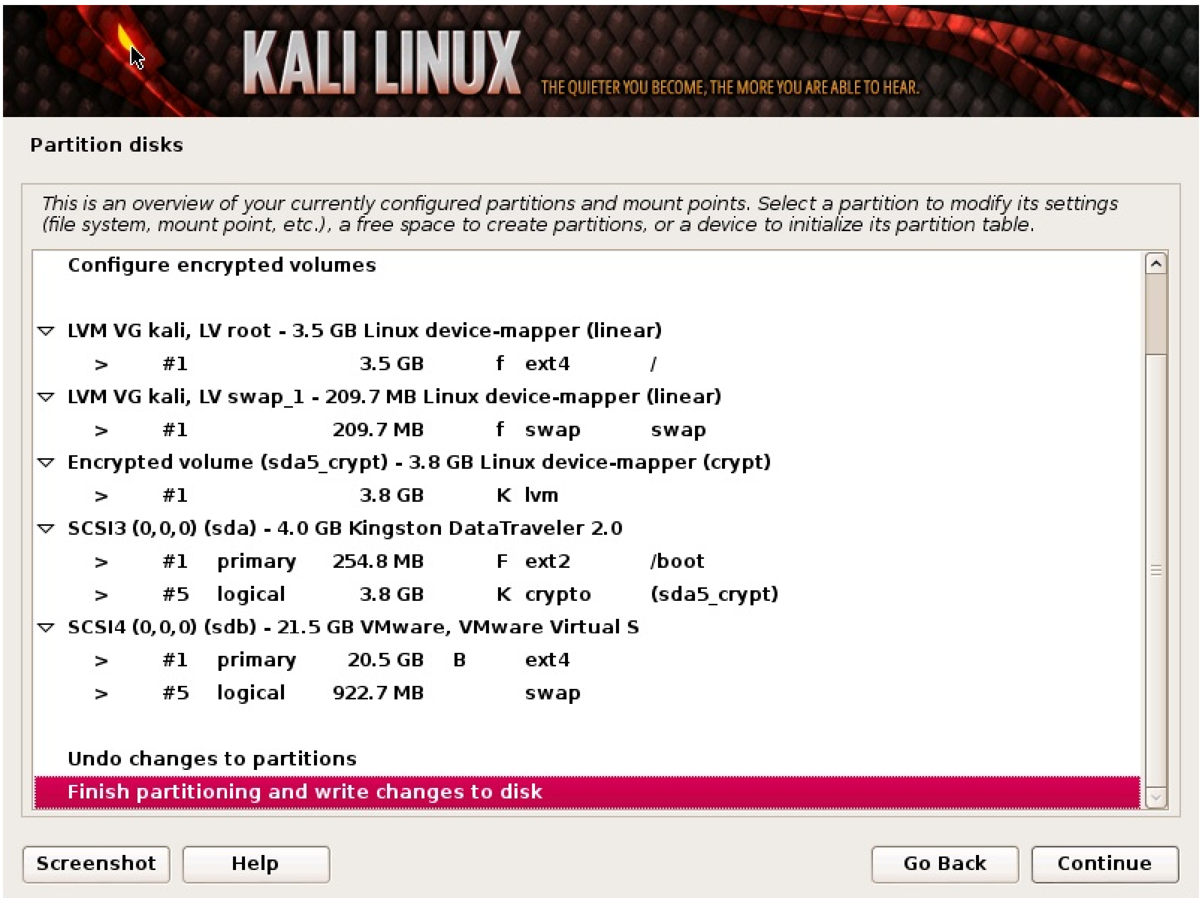
6. 安装器会检测硬盘,并提供4个选项.加密LVM安装应选择"**Guided – use entire disk and set up encrypted LVM(使用全盘LVM加密卷)**".如下图所示.



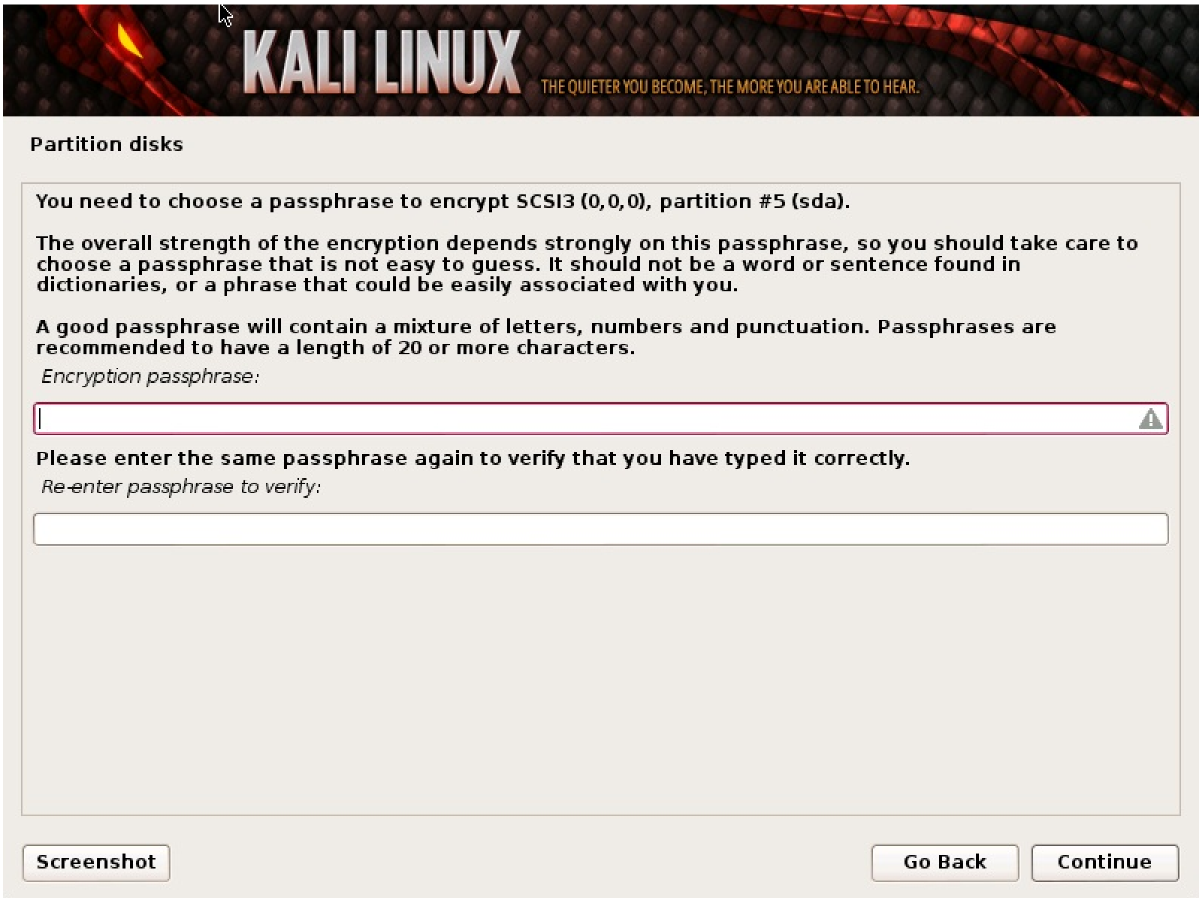
7. 选择安装Kali的目标驱动器.在此例中我们选择一块U盘作为目标驱动器.我们将用这块U盘来启动加密的Kali.



8. 确认你的分区结构并继续安装.

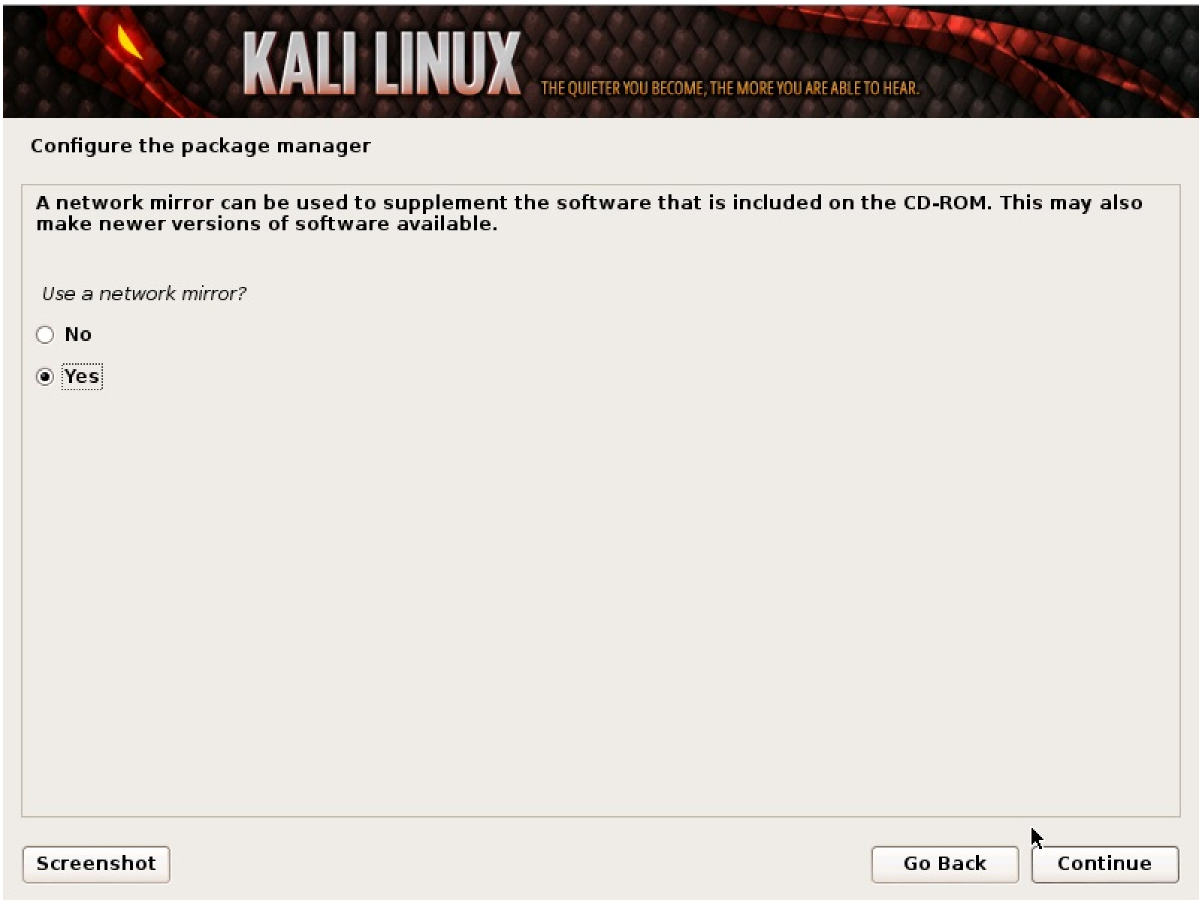


9. 然后,你将被要求输入一个加密密码.你必须记住此密码并在每次启动Kali时输入.



10. 配置网络Mirrors.Kali使用中心源发布软件.在必要的时候你需要输入适当的代理信息.

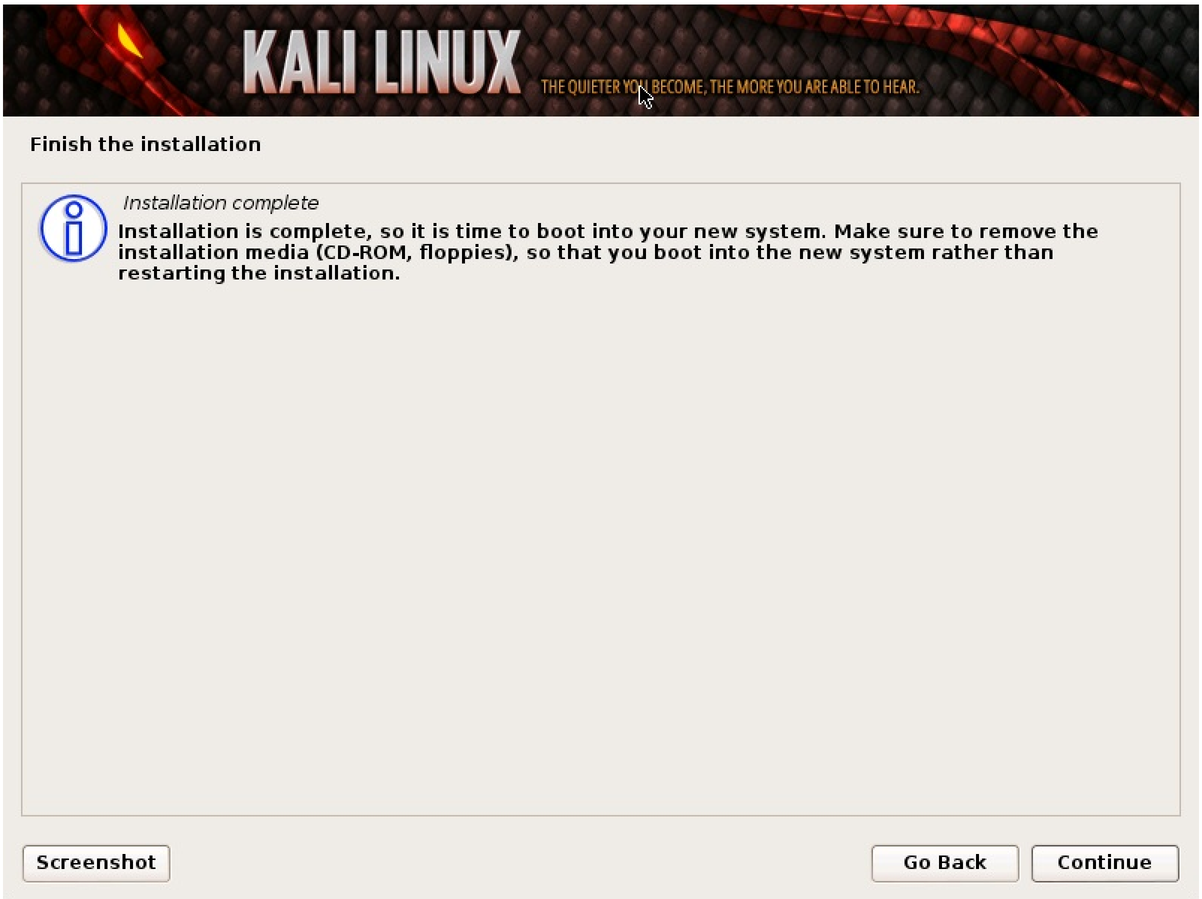
    注意!如果你选择了"NO",你将不能从Kali源安装软件.



11. 下一步安装GRUB.



12. 最后,点击*Continue(继续)*来重启系统,进入全新安装的Kali.如果你安装的目标驱动器是U盘,确认BIOS中已设置为从U盘启动.你将在每次启动时输入先前设置的加密密码.



完成安装

现在你已经完成了Kali Linux的安装,是时候定制你的系统了.官方网站上的Kali常见问题里有更多信息,你还会在用户论坛里找到更多的小技巧.

Kali和Windows双引导

Kali和Windows双引导

把Kali和Windows装在一起很有用.然而,你要谨慎的安装.首先确保你已经备份了你电脑里的重要数据.因为我们要修改你的硬盘,所以你应该把数据备份到别的媒介.一旦你完成了备份,我们推荐你阅读硬盘安装Kali Linux,以了解Kali的基础安装过程.

此例,我们将把Kali Linux和硬盘唯一的Windows 7系统装在一起.我们开始重新给WIndows分区划分分区大小,缩小Windows分区的容量,以便把Kali Linux安装到新建的空分区.

下载Kali Linux刻录到DVD光盘, 或者准备一块Kali linux Live U盘作为安装媒介.如果你的电脑没有DVD光驱或USB端口,请参考网络安装Kali Linux.硬件要求:

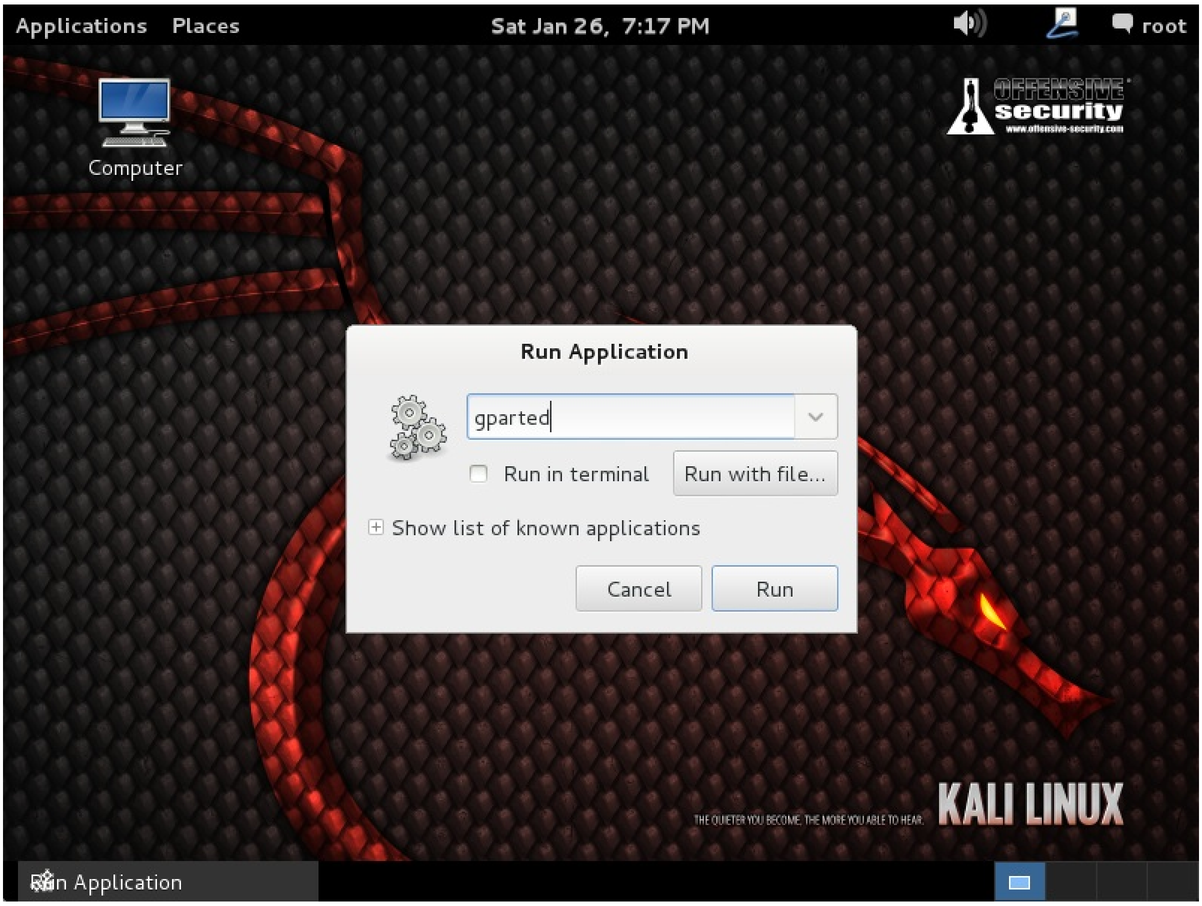
- Windows至少有8G的剩余空间
- 支持CD-DVD / USB引导

准备安装

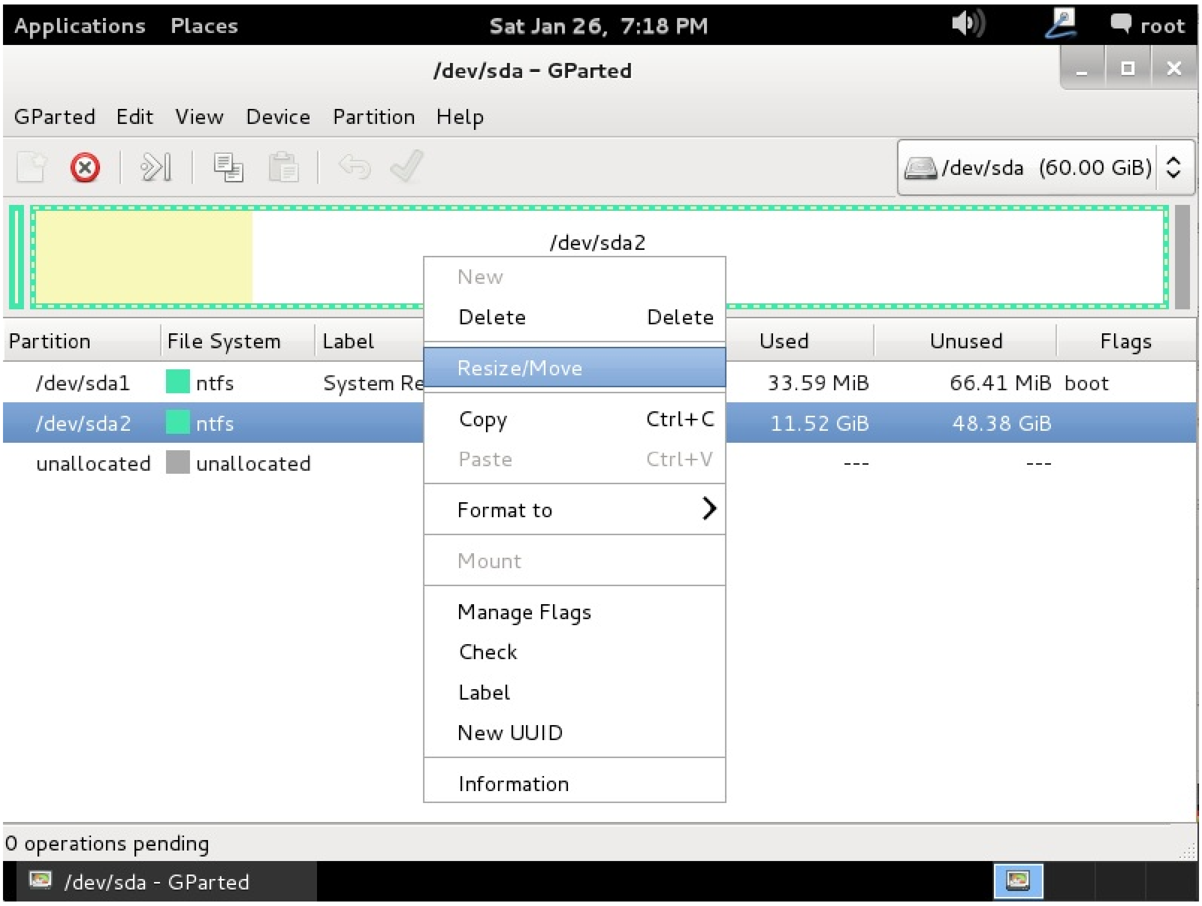
1. 下载Kali Linux.
2. 刻录Kali Linux DVD盘或制作Kali Linux Live U盘.
3. 确保你的电脑BIOS设置了从CD/USB引导.

双系统安装过程

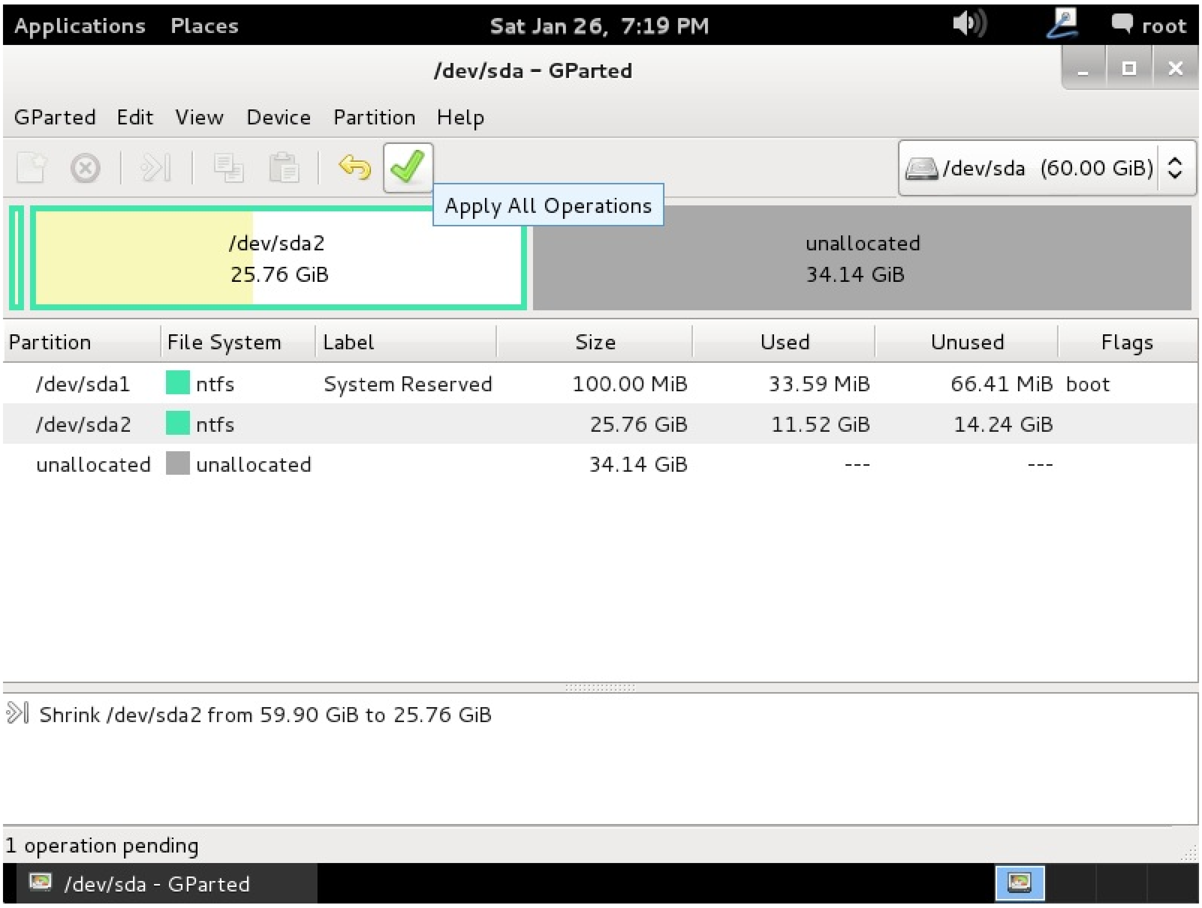
1. 开始安装,从你选择的安装媒介启动. 你会看到Kali的引导界面.选择*Live*,然后你会进入到Kali Linux桌面.
2. 使用用户名**root**,和密码**toor**登录.下一步运行**gparted**程序.我们将用**gparted**缩小windows分区的大小以提供足够的空间安装Kali.



3. 选择Windows分区.根据你的系统情况选择,此例选择较大的第二个分区.此例中有两个分区,第一个分区是系统恢复分区,实际上Windows安装在/dev/sda2.重新调整Windows分区的大小预留(最小8GB)空间给Kali Linux.

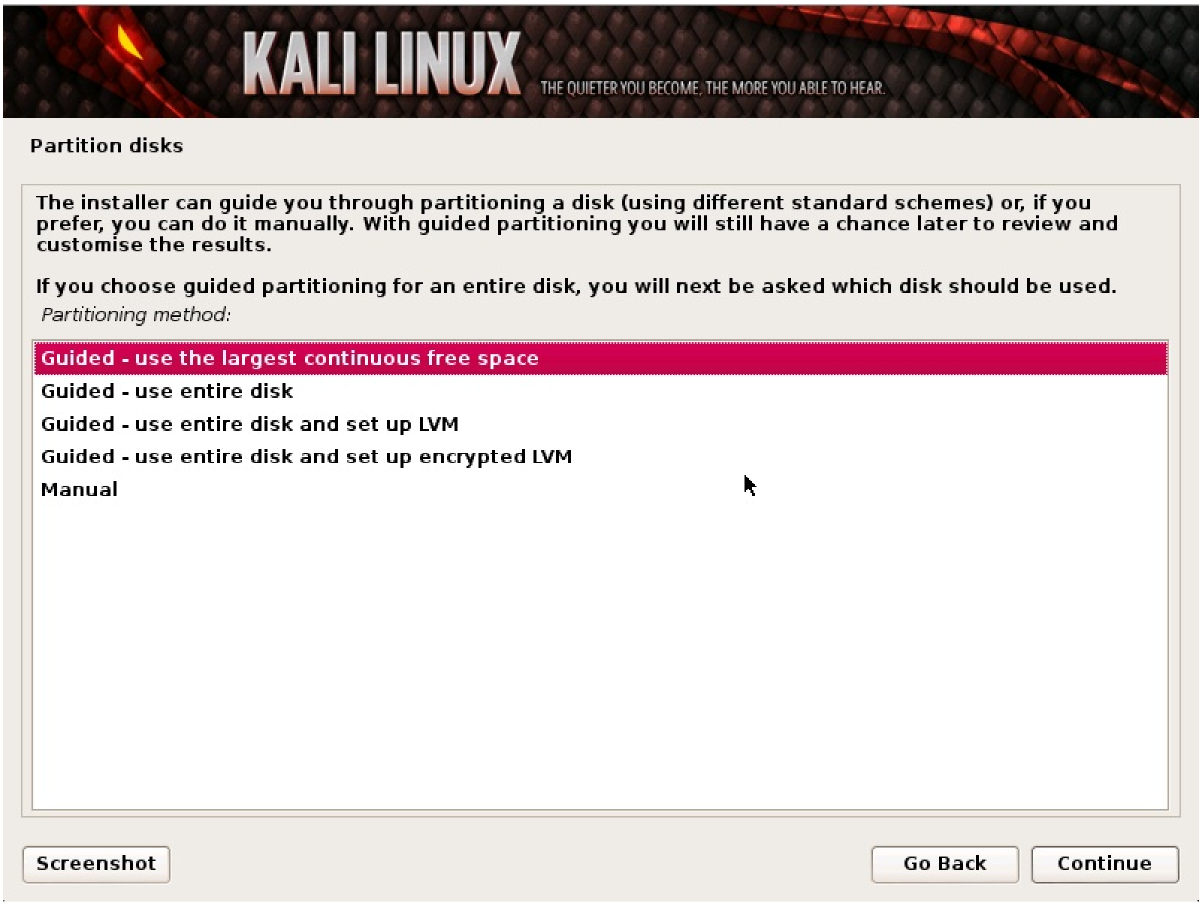


4. 重新分区之后.确保点击了硬盘的"Apply All Operations"(应用所有操作).退出**gparted**并重启.



Kali Linux安装步骤

1. 安装步骤和之前的硬盘安装Kali Linux,类似,除了分区的时候选"Guided – use the largest continuous free space"(上文中用**gparted**创建的分区).



2. 安装完毕,重启.你会看见GRUB的启动菜单有Kali 和 Windows启动项.



安装后

现在你已经完成了Kali Linux的安装,是时候定制你的系统了.官方网站上的Kali常见问题里有更多信息,你还可以在用户论坛里找到更多的小技巧.

硬盘安装Kali Linux

Kali Linux安装条件

安装Kali Linux到你的电脑过程很简单.首先你需要兼容的电脑硬件. Kali支持i386, amd64, 和ARM (armel和armhf) 平台.最低硬件要求如下,更好的硬件性能会更好. i386镜象默认使用PAE内核,所以你能在大于4GB内存的机器运行它.下载Kali Linux然后刻录DVD盘,或者准备好一块Kali Linux Live U盘作为安装媒介.如果你的电脑没有DVD光驱或者USB端口, 请参考Kali Linux网络安装.

安装条件

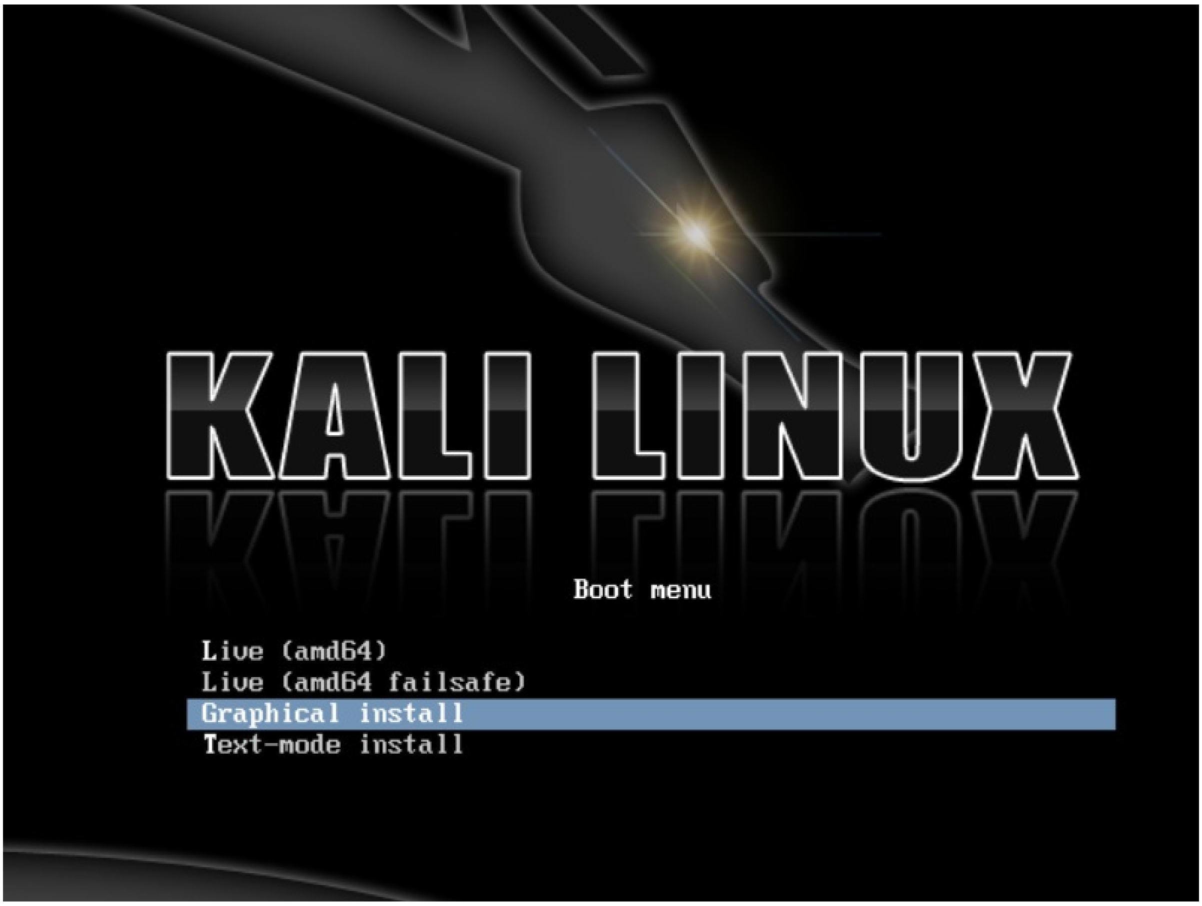
- 安装Kali Linux最少8G硬盘可用空间.
- i386和amd64架构,最低512MB内存.
- CD-DVD光驱/支持USB引导

准备安装

1. 下载Kali linux.
2. 把Kali Linux刻录到DVD盘或制作Kali Linux镜像U盘.
3. 确认你电脑的BIOS设置了从CD/USB引导.

Kali Linux安装步骤

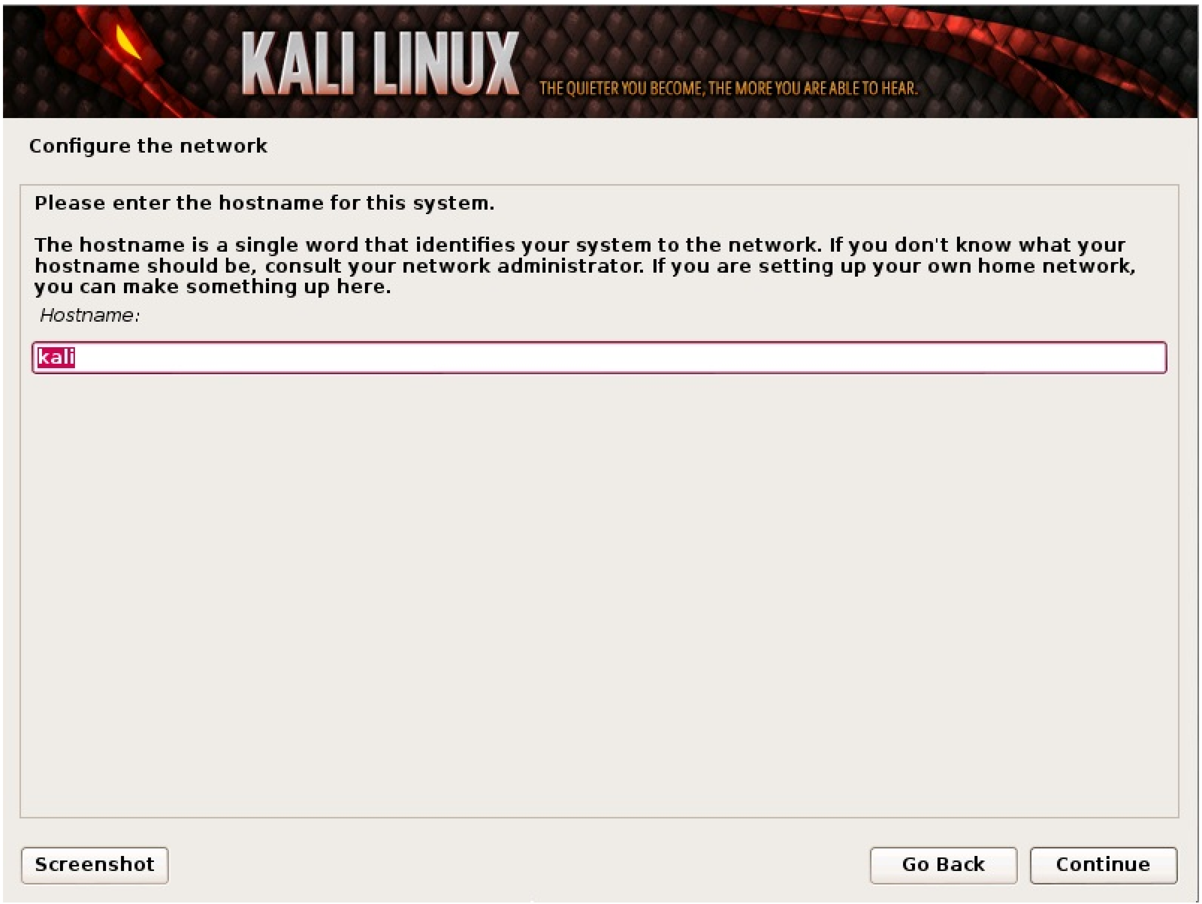
1. 开始安装,从你选择的安装媒介启动. 你会看到Kali的引导界面.选择图形界面安装或者文本模式安装.此处,我们选择图形界面安装.



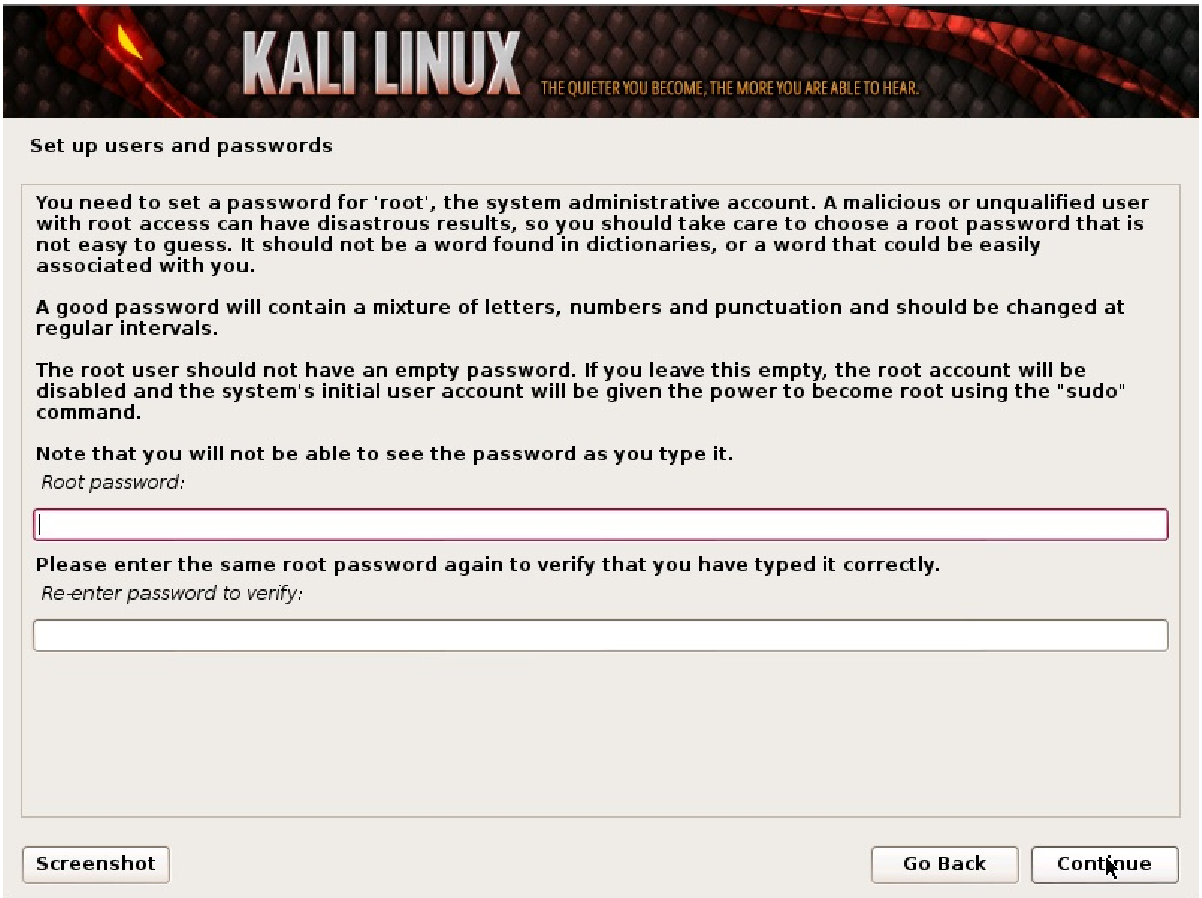
2. 选择你的首选语言和国家.你会被提示为你的键盘配置适当的Keymap.



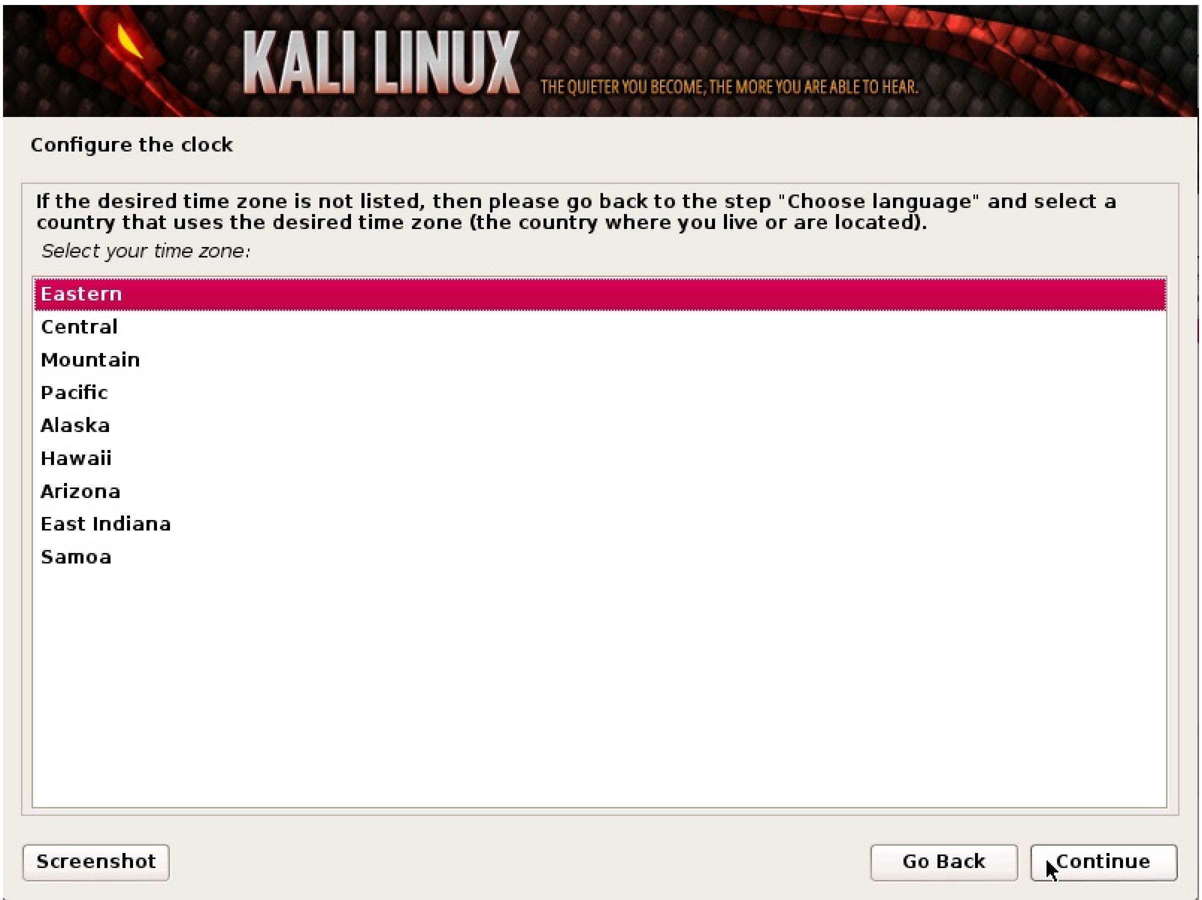
3. 安装器会复制镜象到你的硬盘,探测你的网络接口,然后提示你为你的系统输入主机名.此例,我们输入"Kali"作为主机名.



4. 为root账户输入一个强健的密码,或需要的话创建额外的账户.


KALI LINUX
THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.
Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
Please enter the same root password again to verify that you have typed it correctly.
Re-enter password to verify:
Screenshot
Go Back
Continue

5. 下一步设置时区.

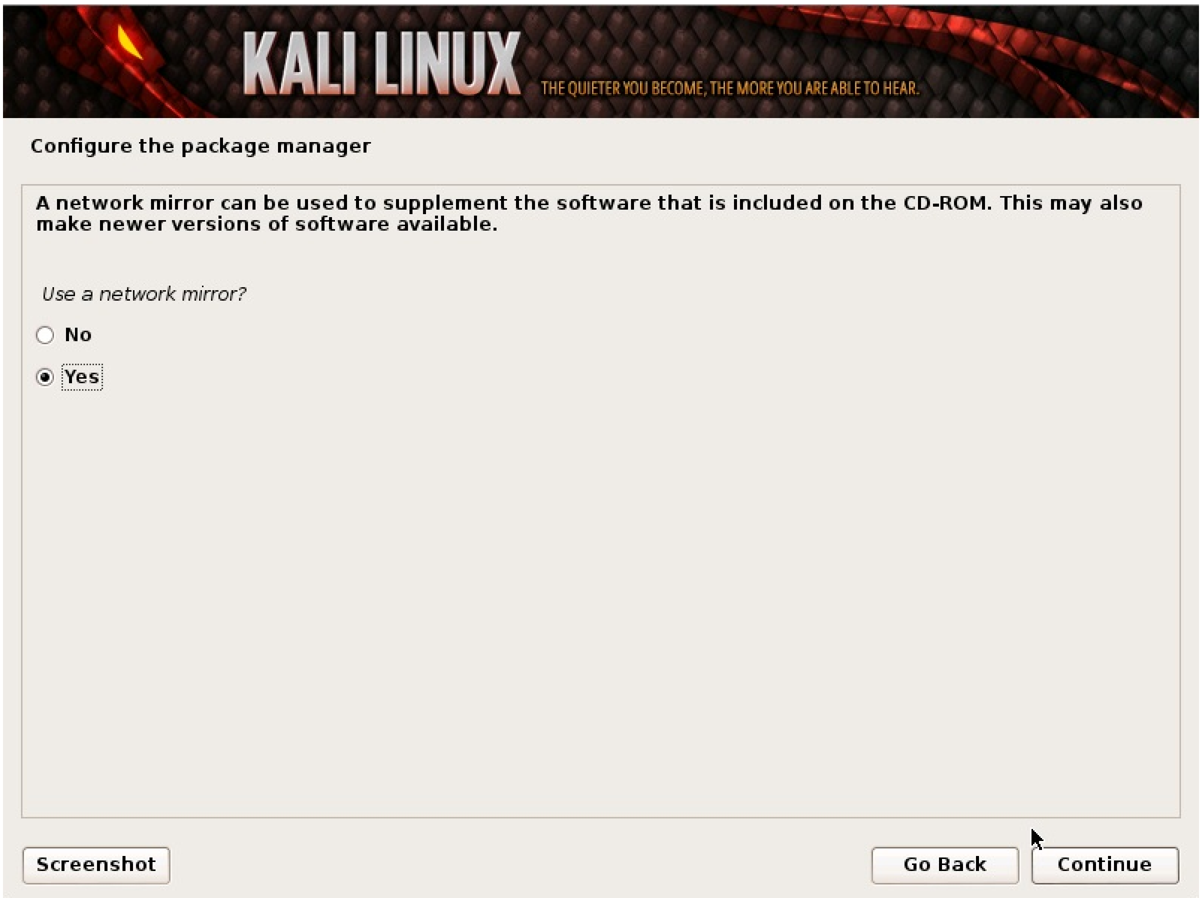

KALI LINUX
THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.
Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
Screenshot
Go Back
Continue

6. 安装器会检测硬盘,并提供4个选项.此例,我们使用电脑的整块硬盘,并且不设置LVM(逻辑卷管理器).高级用户可以使用"手动"分区,配置自己的分区结构.

7. 接着在安装器作出不可逆的改变之前你会有机会检查硬盘配置.在你点击继续按钮后,安装器将开始工作,并且安装也快接近尾声.

8. 配置网络Mirrors.Kali使用中心源发布软件.在必要的时候你需要输入适当的代理信息.

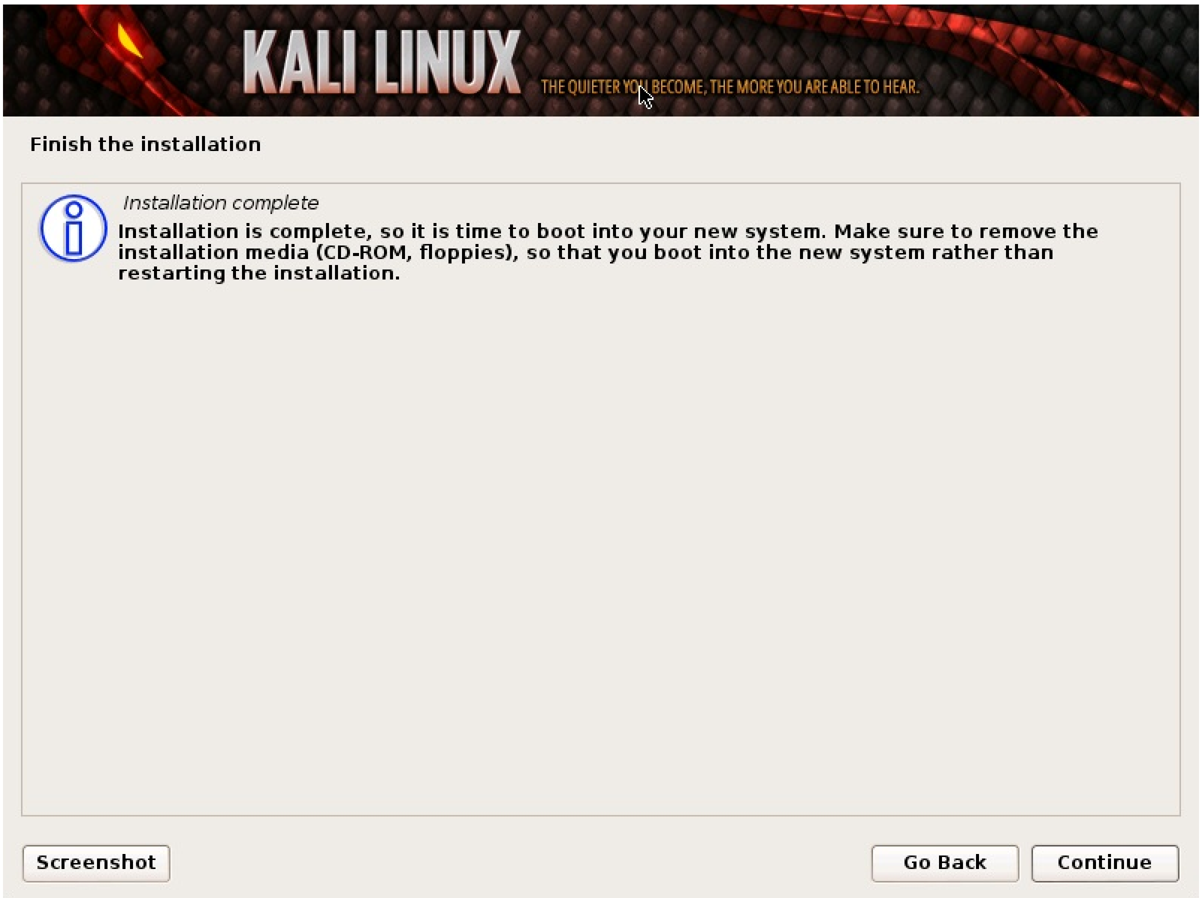
   注意!如果你选择了"NO",你将不能从Kali源安装软件.

9. 下一步安装GRUB.



10. 最后,点击继续来重启系统,进入全新安装的Kali.



安装后

现在你已经完成了Kali Linux的安装,是时候定制你的系统了.官方网站上的Kali常见问题里有更多信息,你还会在用户论坛里找到更多的小技巧.

04. 通过网络安装Kali Linux

05. Kali Linux常见问题

Virtual Box的Kali Linux虚拟机

如果你想在VirtualBOX里安装Kali Linux,为了能够顺利安装功能增强工具,请参考如下的指南.

建议使用最新版的VirtualBOX,因为可以提升用户体验,包括兼容性的提高,软件核心和客户端功能增强工具的稳定性的增强.

在Virtual Box的Kali Linux虚拟机安装增强工具

为了整合鼠标和屏幕以及与你的宿主机共享目录,你应该安装VirtualBox增强功能工具.

启动Kali Linux虚拟机后,打开一个终端然执行如下命令来安装Linux内核头文件.

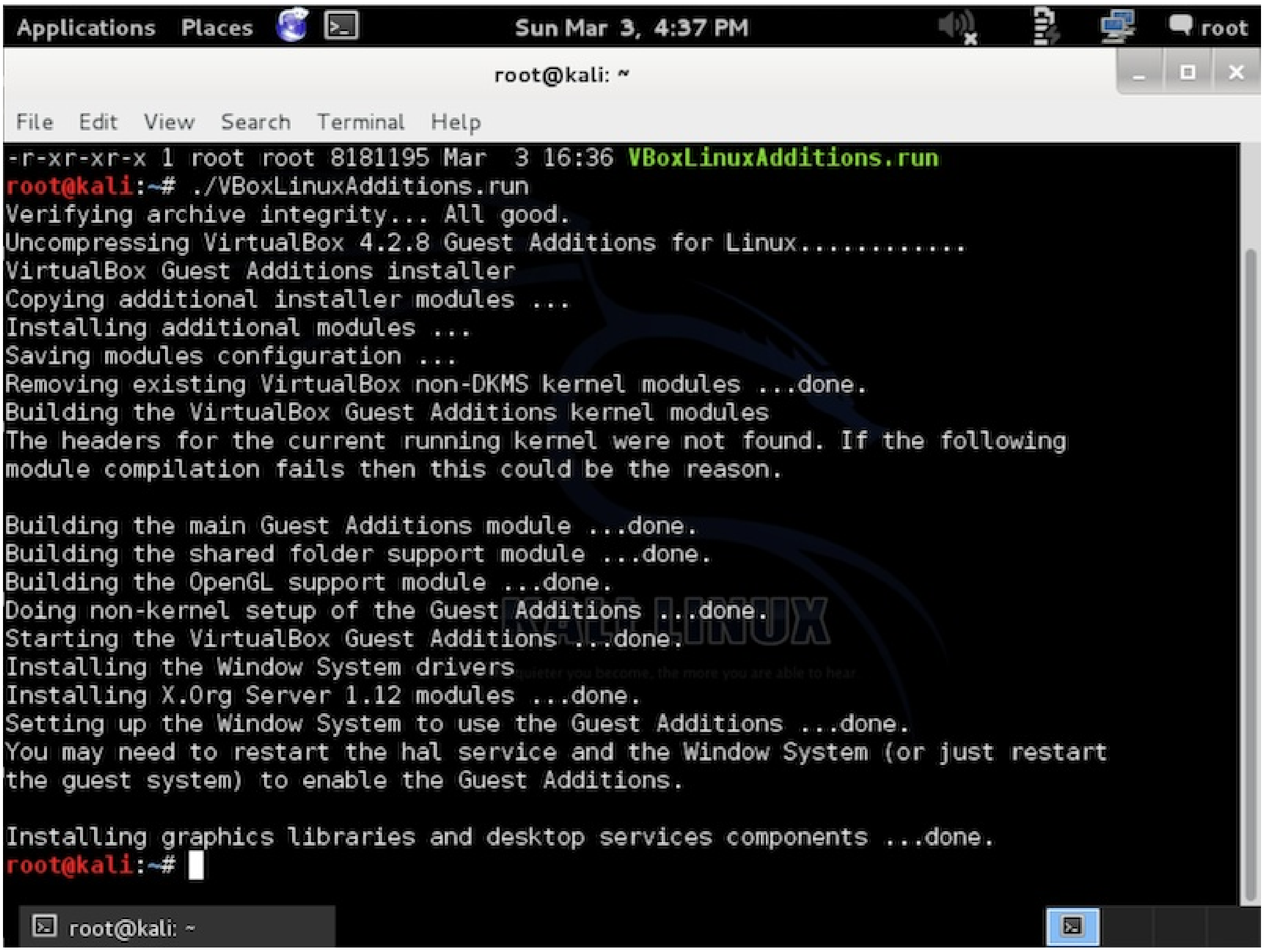
```
apt-get update && apt-get install -y linux-headers-$(uname -r)
```

安装完后,从VirtualBox菜单的"Install Guest Additions"选择'Devices'来挂载客户端功能增强的ISO到虚拟机的CD光驱.提示自动运行CD时,点击取消按钮.



在终端窗口,复制虚拟机CD-Rom里的VboxLinuxAdditions.run这个文件到本地目录,确认有可执行权限,然后运行该文件开始安装.

```
cp /media/cd-rom/VBoxLinuxAdditions.run /root/
chmod 755 /root/VBoxLinuxAdditions.run
cd /root
./VBoxLinuxAdditions.run
```



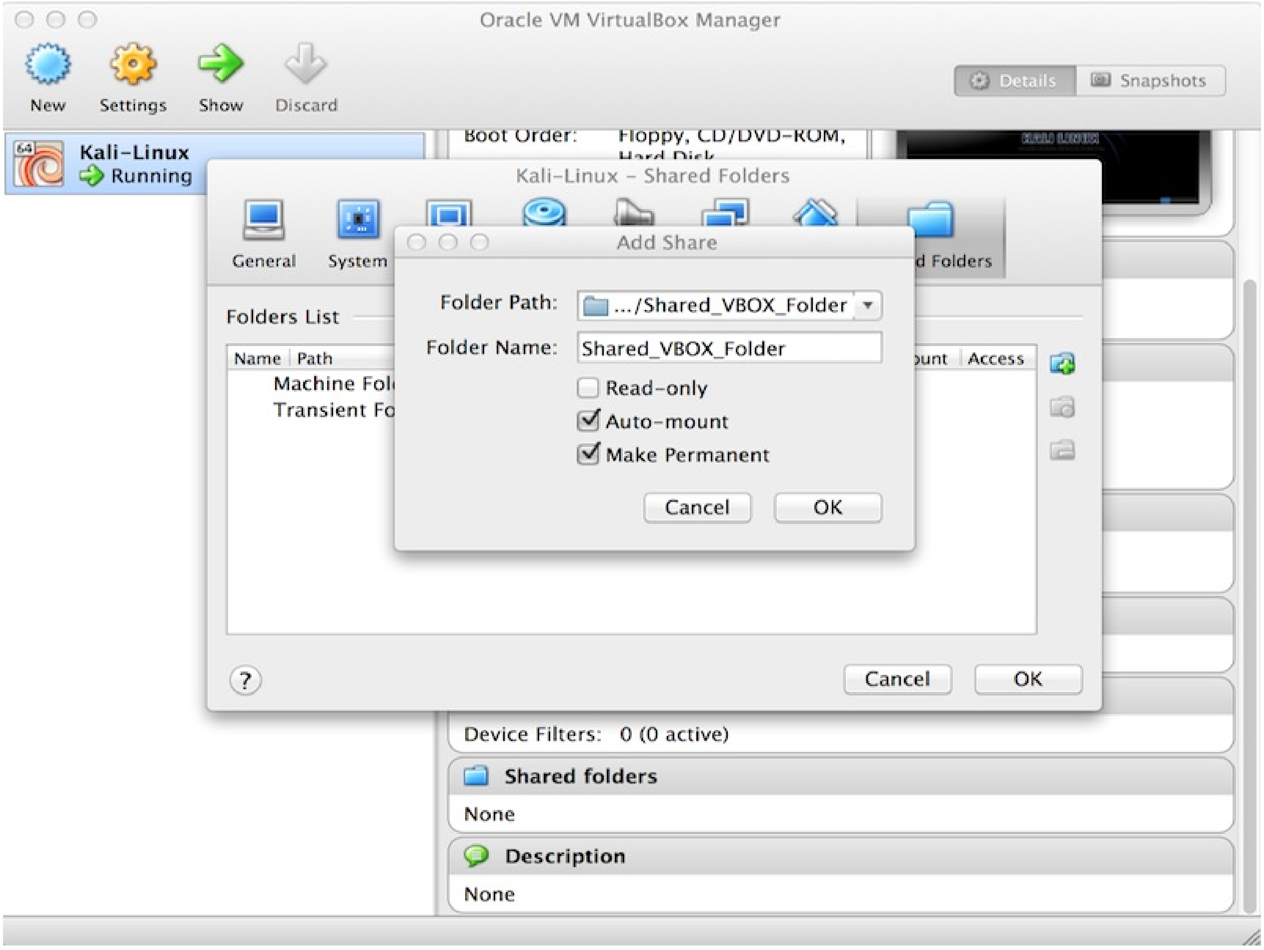
功能增强工具安装好后重启Kali Linux虚拟机.鼠标和屏幕整合好了,也可以与宿主机共享目录了.

创建宿主机的共享目录

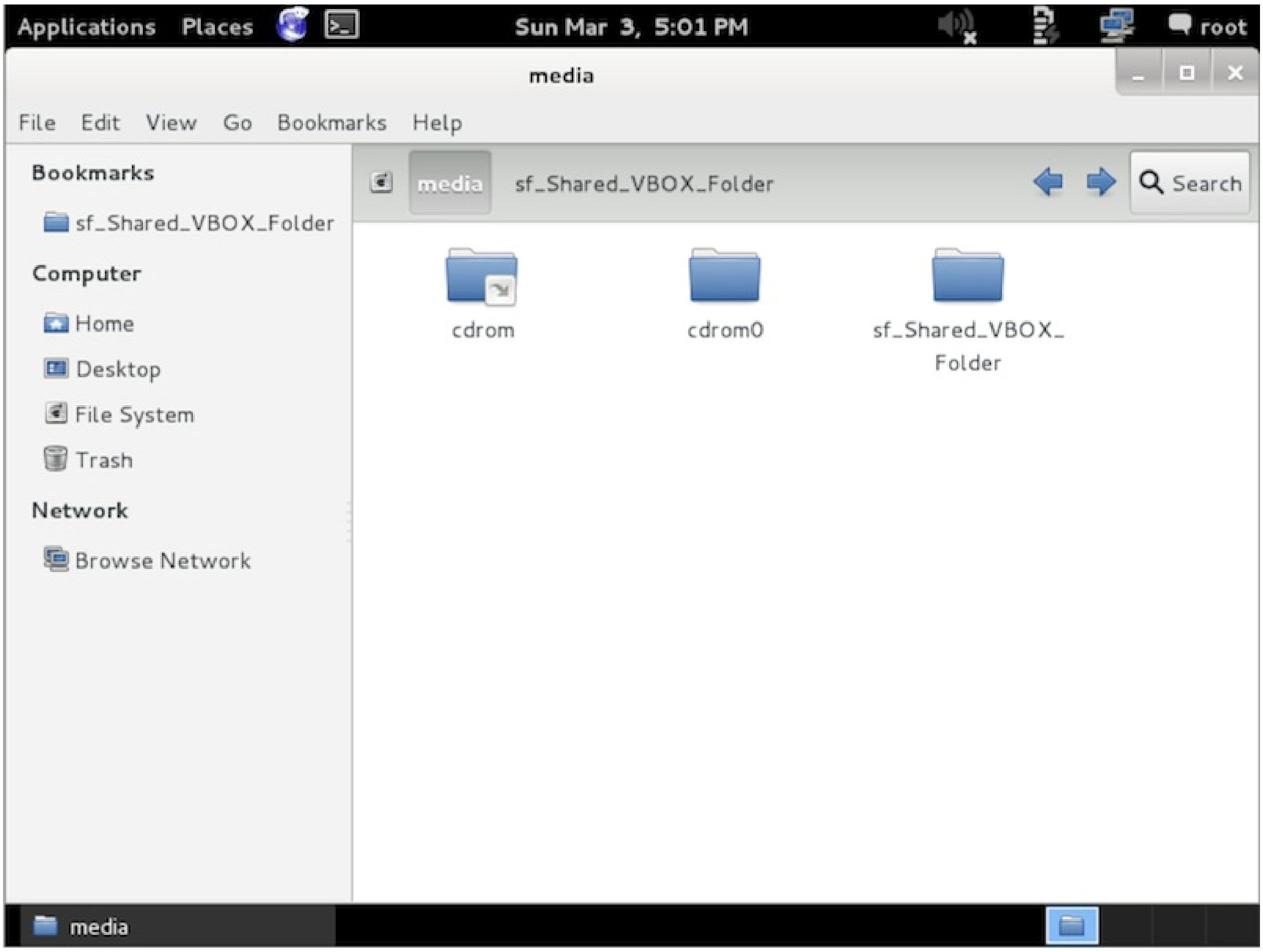
为了共享宿主机上的目录给你的Kali Linux虚拟机,有一些步骤要完成.

在虚拟机管理器,选择你的Kali Linux虚拟机然后点击右键菜单的'Shared Folders'.会弹出一个用于添加共享目录的窗口.在这个窗口里点击图标来添加一个目录.

在Folder Path文本框,显示着共享文件夹的路径,或点击下拉菜单箭头来浏览宿主机的系统.勾选Auto-mount(自动挂载)'和'Make Permanent(永久)'复选框,当有提示时点击OK按钮.



现在共享目录会出现在media目录里.为了可以方便的进入到这个目录你可以创建一个书签或者链接.


Applications
Places
Sun Mar 3, 5:01 PM
root
media
File
Edit
View
Go
Bookmarks
Help
Bookmarks
sf_Shared_VBOX_Folder
Computer
Home
Desktop
File System
Trash
Network
Browse Network
media
sf_Shared_VBOX_Folder
Search
cdrom
cdrom0
sf_Shared_VBOX_Folder
media

运行 Metasploit Framework

依照Kali Linux网络服务策略,Kali没有自动启动的网络服务,包括数据库服务在内.所以为了让Metasploit以支持数据库的方式运行有些必要的步骤.

启动Kali的PostgreSQL服务

Metasploit 使用PostgreSQL作为数据库,所以必须先运行它.

```
service postgresql start
```

你可以用**ss -ant**的输出来检验PostgreSQL是否在运行,然后确认5432端口处于listening状态.

```
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 128 :::22 :::*
LISTEN 0 128 *:22 *:*
LISTEN 0 128 127.0.0.1:5432 *:*
LISTEN 0 128 ::1:5432 :::*
```

启动Kali的Metasploit服务

随着PostgreSQL的启动和运行,接着我们要运行Metasploit服务.第一次运行服务会创建一个msf3数据库用户和一个叫msf3的数据库.还会运行Metasploit RPC和它需要的WEB 服务端.

```
service metasploit start
```

在Kali运行msfconsole

现在PostgreSQL 和 Metasploit服务都运行了,可以运行 **msfconsole** ,然后用 **db_status** 命令检验数据库的连通性.

```
msfconsole
```

```
msf > db_status
[*] postgresql connected to msf3
msf >
```

配置Metasploit随系统启动运行

如果你想PostgreSQL和Metasploit在开机时运行,你可以使用**update-rc.d**启用服务.

```
update-rc.d postgresql enable
```

```
update-rc.d metasploit enable
```

Kali虚拟机安装VMware Tools

我们建议你自己创建一台Kali Linux的VMware虚拟机,而不是使用我们预先提供的VMware镜象,进行如下的操作以便在Kali虚拟机成功安装VMware Tools.你可以选择安装**open-vm-tools**,或自带的**VMWare tools**.

安装open-vm-Tools

这可能是在Kali虚拟机里实现"VMware Tools"功能最容易的方法.

```
apt-get install open-vm-tools
```

在Kali里安装VMware Tools

如果open-vm-tools不能用,或者你更偏向于使用VMware Tools,开始安装一些VMware Tools安装器需要的包:

```
apt-get install gcc make linux-headers-$(uname -r)
ln -s /usr/src/linux-headers-$(uname -r)/include/generated/uapi/linux/version.h /usr/src/
```

下一步,通过点击菜单里的"Install VMware Tools"挂载VMware Tools的ISO.虚拟机的光驱连接到VMware Tools ISO后,我们挂载驱动器然后复制VMware Tools安装器到/tmp/目录下.

```
mkdir /mnt/vmware
mount /dev/cdrom /mnt/vmware/
cp -rf /mnt/vmware/VMwareTools* /tmp/
```

最后,进到/tmp/目录,解压缩然后开始安装:

```
cd /tmp/
tar zxpf VMwareTools-*.tar.gz
cd vmware-tools-distrib/
./vmware-tools-install.pl
```

照着上面的命令,VMware Tools就安装好了.

VMware里鼠标移动很慢

如果在Kali Linux的VMware虚拟机里,你的鼠标移动很慢或者反应很迟钝.尝试在Kali虚拟机里安装**xserver-xorg-input-vmmouse**这个包.

```
apt-get install xserver-xorg-input-vmmouse
reboot
```

VMWare Tools不能编译!

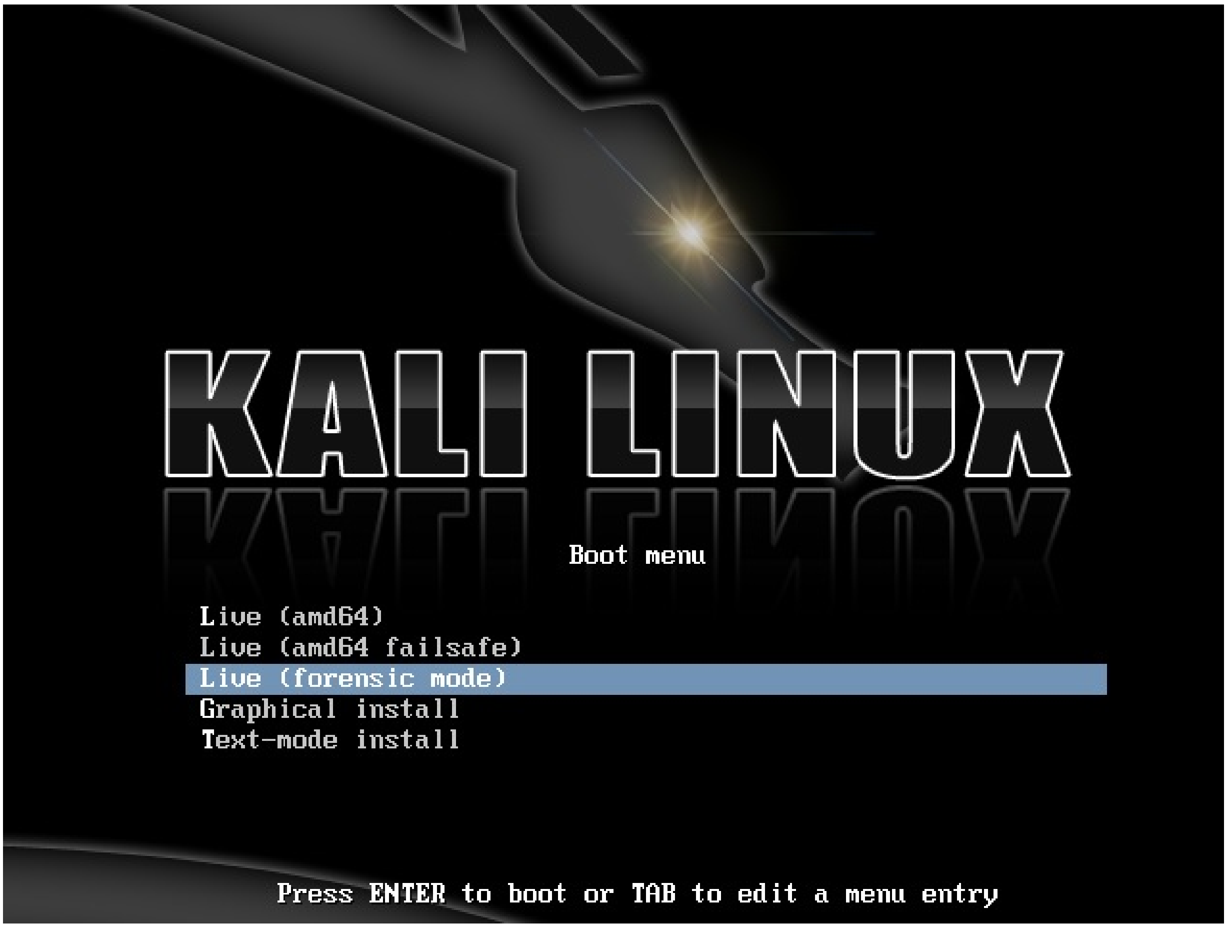
这是个经常折磨我们不幸的事实,例如Kali Linux用了VMware还没有支持的太新的内核.有时,可能需要在VMware社区寻找"兼容的VMware Tools补丁".

已知问题

截自2013年3月2日为止.VMware Tools已经在3.7内核编译通过,除了共享文件夹模块不能正常工作外.已经有补丁可以解决这个问题.

Kali Linux电子取证模式

BackTrack Linux引入了"Forensic Boot"启动选项,BackTrack 5里也有,现在Kali Linux里依然有这个选项.由于Backtrack Linux的广泛传播,"Forensic Boot"也被证明是非常的流行.许多人都备着Kali Linux，以便在需要取证时方便的用上.它集成了流行的开源取证工具,Kali是在你需要做开源取证工作时非常趁手的工具.



启动到"forensic boot"模式后,你会发现这个模式有一些非常重要的改变.

1. 首先,不会触及到内部硬盘.这意味着SWAP分区和内部硬盘分区不会被自动挂载.为了验证这一点,我们找来一个标准系统然后拆掉硬盘.用商业的取证软件获取这块硬盘的Hash.然后再把它接回到电脑上用Kali的取证启动模式启动.在使用了Kali一段时间后,我们关机,再次拆除硬盘并获取它的Hash.两个Hash一致,表明了硬盘没有任何改变.

2. 其次,很重要的一点,我们修改了"自动挂载任意可卸载媒体"为禁用.所以插入U盘,光盘,等等时将不会被自动挂载.这个想法的由来很简单:用户不操作不会改变任何媒介.产生改变都是用户所为.

如果你有兴趣在现实中用Kali任意类型的取证,我们希望你不要以为我们只是在危言耸听.不管在什么情况下使用取证工具都应该确保知道它们在做什么.

最后,鉴于Kali一直专注于容纳各种优秀的开源渗透测试软件.也许我们漏掉了你最喜欢的开源工具,如果是这种情况的话,请给我们反馈! 我们一直着眼于寻找和集成高质量的开源工具以让Kali系统变的更好.

06. Kali Linux ARM文档

在MK/SS808上安装Kali ARM



SS808 ARM Devices (rk3306)

SainSmart SS808是一种基于**rockchip**芯片的ARM设备.它搭载了一个双核1.6GHz的A9处理,还有1G内存,能很好的运行Kali.

存储Kali在SS808 – 简单版

如果你想安装Kali到你的SS808,按照下列步骤:

1. 一张至少8G的高速SD卡,最好是Class 10的.
2. 在我们的下载区下载Kali Linux SS808镜象.
3. 用**dd**命令把镜象文件写入到SD卡.本例中,假设存储设备的设备块名是/dev/sdb,使用的是SS808镜像.如果有变**,**自行更改**.**
4. 把MK808-Finless-1-6-Custom-ROM下载到Windows系统的电脑并解压这个zip文件.
5. 阅读MK808 Finless ROM工具的README,然后安装需要的Windows驱动.
6. 运行Finless ROM刷机工具,确认下面有提示“Found RKAndroid Loader Rock USB”.然后在列表中取消kernel.img和recovery.img选项,然后开始刷机.
7. 然后下一步用kail的kernel.img和recovery.img覆盖Finless ROM目录下的kernel.img和recovery.img.
8. 在Finless ROM工具里,确认只选了“kernel.img”和“recovery.img”,然后再刷一次.
9. 把microSD卡插入到SS808然后启动.

警告**!**这步将会擦除SD卡内的数据,如果选择了错误的存储设备,会导致硬盘数据丢失..

```
dd if=kali-SS808.img of=/dev/sdb bs=1M
```

这步需要的时间取决于你的USB存储设备的速度和镜象大小.dd命令完成,插入SD卡到SS808再启动.你将可以用（root/toor）登录,然后用**startx**启动图形界面.就这样,完成了!

SS808上的Kali – 复杂版

如果你是个开发者,你想修改Kali Linux SS808的镜象,包括修改内核配置,查阅我们的文章“定制MK/SS808镜像”.

在三星Chromebook安装Kali



三星ARM chromebook是一台超级本.很具挑战性,但我们的Kali镜像在Chromebook上运运行得很好.

我们的Chromebook Kali镜像包含两种引导分区,其中一种的内核强制从SD卡引导,另一种的内核强制从USB引导.根据你使用哪种类型的USB存储媒介,在dd命令把镜像克隆到USB设备后,确定如何给引导分区标记更高的优先权,本指南的最后阶段将会提及.

Kali在Chromebook上 – 用户指南

如果你想安装Kali到你的Samsung ARM Chromebook,按照下列步骤:

1. 准备一块高速的8G SD卡或U盘.
2. 把Chromebook设置成开发者模式.
3. 从我们的downloads下载Kali的Samsung ARM Chromebook镜像.
4. 用**dd**命令把镜象文件克隆到SD卡.本例中,假设存储设备的设备块名是/dev/sdb.根据情况,自行更改.

警告**!**这步将会擦除SD卡内的数据,如果选择了错误的存储设备,会导致硬盘数据丢失..

```
dd if=kali-chromebook.img of=/dev/sdb bs=512k
```

这步需要的时间取决于USB存储设备的速度和镜象的大小.

就是这里,你要给分区1或是分区2标记更高的优先权.数字大则有更高的优先权.如下的例子将把第一个分区(用-i参数)的优先权设置成10,因为我们要从SD卡引导.

```
cgpt repair /dev/sdb
cgpt add -i 1 -S 1 -T 5 -P 10 -l KERN-A /dev/sdb
cgpt add -i 2 -S 1 -T 5 -P 5 -l KERN-B  /dev/sdb
```

使用**cgpt show**命令查看分区的列表和引导顺序.

```
root@kali:~# cgpt show /dev/sdb
       start        size    part  contents
           0           1          PMBR
           1           1          Pri GPT header
           2          32          Pri GPT table
        8192       32768       1  Label: "KERN-A"
                                  Type: ChromeOS kernel
                                  UUID: 63AD6EC9-AD94-4B42-80E4-798BBE6BE46C
                                  Attr: priority=10 tries=5 successful=1
       40960       32768       2  Label: "KERN-B"
                                  Type: ChromeOS kernel
                                  UUID: 37CE46C9-0A7A-4994-80FC-9C0FFCB4FDC1
                                  Attr: priority=5 tries=5 successful=1
       73728     3832490       3  Label: "Linux filesystem"
                                  Type: 0FC63DAF-8483-4772-8E79-3D69D8477DE4
                                  UUID: E9E67EE1-C02E-481C-BA3F-18E721515DBB
   125045391          32          Sec GPT table
   125045423           1          Sec GPT header
root@kali:~#
```

dd操作完成后,插入SD卡/U盘启动Chromebook(不要插在蓝色的USB口!).在开发者引导提示里按CTRL + ALT + U引导进入到Kali Linux.用(root / toor)登录到Kali,然后运行**startx**.就这样,大功告成!!

Kali在Chromebook上 – 开发指南

如果你是一个开发者,想折腾Kali 三星Chromebook的镜像,包括修改内核配置或更具冒险精神的尝试,请查阅我们的文章[定制Chromebook内核/镜像].

07. Kali Linux开发

定制Raspberry Pi镜像

本文针对开发者描述何如创建一个定制的**Raspberry Pi ARM**版**Kali Linux**镜像的方法.如果你只是想安装Kali镜像,请查阅我们的文章“安装Kali Linux ARM版到Raspberry Pi”.

01. 创建Kali rootfs

创建一个**armel**架构的如Kali文档中所述的Kali rootfs.最后生成的rootfs将位于**~/arm-stuff/rootfs/kali-armel**目录.

02. 创建镜像文件

然后,我们创建用于存放我们Raspberry Pi rootfs和boot镜像的物理镜像文件.

```
apt-get install kpartx xz-utils sharutils
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p images
cd images
dd if=/dev/zero of=kali-custom-rpi.img bs=1MB count=5000
```

03. 分区并挂载镜像文件

```
parted kali-custom-rpi.img --script -- mklabel msdos
parted kali-custom-rpi.img --script -- mkpart primary fat32 0 64
parted kali-custom-rpi.img --script -- mkpart primary ext4 64 -1
```

```
loopdevice=`losetup -f --show kali-custom-rpi.img`
device=`kpartx -va $loopdevice| sed -E 's/.*(loop[0-9])p.*/1/g' | head -1`
device="/dev/mapper/${device}"
bootp=${device}p1
rootp=${device}p2

mkfs.vfat $bootp
mkfs.ext4 $rootp
mkdir -p root
mkdir -p boot
mount $rootp root
mount $bootp boot
```

04. 复制和修改Kali rootfs

```
rsync -HPavz /root/arm-stuff/rootfs/kali-armel/ root
echo nameserver 8.8.8.8 > root/etc/resolv.conf
```

05. 编译Raspberry Pi内核和模块

如果你不是以ARM硬件作为开发环境,需要搭建ARM交叉编译环境来编译ARM内核和模块.完成后,执行如下命令.

```
cd ~/arm-stuff
mkdir -p kernel
cd kernel
git clone https://github.com/raspberrypi/tools.git
git clone https://github.com/raspberrypi/linux.git raspberrypi
cd raspberrypi
export ARCH=arm
export CROSS_COMPILE=~/arm-stuff/kernel/toolchains/arm-eabi-linaro-4.6.2/bin/arm-eabi-
make bcmrpi_cutdown_defconfig
# configure your kernel !
make menuconfig
make -j$(cat /proc/cpuinfo|grep processor|wc -l)
make modules_install INSTALL_MOD_PATH=~/arm-stuff/images/root
cd ../tools/mkimage/
python imagetool-uncompressed.py ../../raspberrypi/arch/arm/boot/Image
```

```
cd ~/arm-stuff/images
git clone git://github.com/raspberrypi/firmware.git rpi-firmware
cp -rf rpi-firmware/boot/* boot/
rm -rf rpi-firmware

cp ~/arm-stuff/kernel/tools/mkimage/kernel.img boot/
echo "dwc_otg.lpm_enable=0 console=ttyAMA0,115200 kgdboc=ttyAMA0,115200 console=tty1 root
```

```
umount $rootp
umount $bootp
kpartx -dv $loopdevice
losetup -d $loopdevice
```

使用**dd**工具克隆这个文件到你的SD卡.在本例中,我们假设存储设备在/dev/sdb.请按需修改.

```
dd if=kali-pi.img of=/dev/sdb bs=1M
```

dd操作完成后,卸载并弹出SD卡.然后启动进入到Kali Linux

定制Chromebook镜像

针对开发者,如下的文档描述我们创建个性化的**Kali Linux Samsung chromebook ARM**镜像的方法.如果你想安装预发的Kali image,查阅我们的文档在三星Chromebook安装Kali.

本文档中,我们创建一个镜像(包含两种引导分区) – 一种分区包含了强制从SD卡引导的内核,另一种包含了强制从USB引导的内核.根据你的USB存储媒介的类型,确保你在用dd把镜像克隆到USB设备后(本指南最后的命令),用更高的优先权标志相关的引导分区.

01. 创建Kali rootfs

开始创建我们文档中描述的Kali rootfs使用armhf架构.到文档的最后,在**~/arm-stuff/rootfs/kali-armhf**目录里应该有一个里面包含很多文件的**rootfs**目录.

02. 创建镜像文件

下一步,我们创建用于存放我们Chromebook rootfs和引导镜像的物理镜像文件.

```
apt-get install kpartx xz-utils gdisk uboot-mkimage u-boot-tools vboot-kernel-utils vboot
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p images
cd images
dd if=/dev/zero of=kali-custom-chrome.img bs=1MB count=5000
```

03. 分区和挂载镜像文件

```
parted kali-custom-chrome.img --script -- mklabel msdos
parted kali-custom-chrome.img --script -- mktable gpt
gdisk kali-custom-chrome.img << EOF
x
l
8192
m
n
1

+16M
7f00
n
2

+16M
7f00
n
3

w
y
EOF
```

```
loopdevice=`losetup -f --show kali-custom-chrome.img`
device=`kpartx -va $loopdevice| sed -E 's/.*(loop[0-9])p.*/1/g' | head -1`
device="/dev/mapper/${device}"
bootp1=${device}p1
bootp2=${device}p2
rootp=${device}p3

mkfs.ext4 $rootp
mkdir -p root
mount $rootp root
```

04. 复制和修改Kali rootfs

用**rsync**递归复制先前挂载的Kali rootfs镜像.

```
cd ~/arm-stuff/images/
rsync -HPavz ~/arm-stuff/rootfs/kali-armhf/ root

echo nameserver 8.8.8.8 > root/etc/resolv.conf

mkdir -p root/etc/X11/xorg.conf.d/
cat << EOF > root/etc/X11/xorg.conf.d/50-touchpad.conf
Section "InputClass"
  Identifier "touchpad"
  MatchIsTouchpad "on"
  Option "FingerHigh" "5"
  Option "FingerLow" "5"
EndSection
EOF
```

05. 编译三星Chromium内核和模块

如果你不是使用ARM硬件作为开发环境,为了编译ARM内核和模块你应该先建立ARM交叉编译环境.完成后,用如下命令继续.

获取Chromium内核源代码并放到我们的开发树结构中:

```
cd ~/arm-stuff
mkdir -p kernel
cd kernel
git clone http://git.chromium.org/chromiumos/third_party/kernel.git -b chromeos-3.4 chrom
cd chromeos
```

```
cat << EOF > kernel.its
/dts-v1/;

/ {
    description = "Chrome OS kernel image with one or more FDT blobs";
    #address-cells = <1>;
    images {
        kernel@1{
   description = "kernel";
            data = /incbin/("arch/arm/boot/zImage");
            type = "kernel_noload";
            arch = "arm";
            os = "linux";
            compression = "none";
            load = <0>;
            entry = <0>;
        };
        fdt@1{
            description = "exynos5250-snow.dtb";
            data = /incbin/("arch/arm/boot/exynos5250-snow.dtb");
            type = "flat_dt";
            arch = "arm";
            compression = "none";
            hash@1{
                algo = "sha1";
            };
        };
    };
    configurations {
        default = "conf@1";
        conf@1{
            kernel = "kernel@1";
            fdt = "fdt@1";
        };
    };
};
EOF
```

为内核打补丁,我们以打无线注入补丁为例.

```
mkdir -p ../patches
wget http://patches.aircrack-ng.org/mac80211.compat08082009.wl_frag+ack_v1.patch -O ../pa
wget http://patches.aircrack-ng.org/channel-negative-one-maxim.patch -O ../patches/negati
patch -p1 < ../patches/negative.patch
patch -p1 < ../patches/mac80211.patch
```

配置,然后像下面一样交叉编译Chromium内核.

```
export ARCH=arm
export CROSS_COMPILE=~/arm-stuff/kernel/toolchains/arm-eabi-linaro-4.6.2/bin/arm-eabi-

./chromeos/scripts/prepareconfig chromeos-exynos5
# Disable LSM
sed -i 's/CONFIG_SECURITY_CHROMIUMOS=y/# CONFIG_SECURITY_CHROMIUMOS is not set/g' .config
# If cross compiling, do this once:
sed -i 's/if defined(__linux__)/if defined(__linux__) ||defined(__KERNEL__) /g' include/d

make menuconfig
make -j$(cat /proc/cpuinfo|grep processor|wc -l)
make dtbs
cp ./scripts/dtc/dtc /usr/bin/
mkimage -f kernel.its kernel.itb
make modules_install INSTALL_MOD_PATH=~/arm-stuff/images/root/

# copy over firmware. Ideally use the original firmware (/lib/firmware) from the Chromebo
git clone git://git.kernel.org/pub/scm/linux/kernel/git/dwmw2/linux-firmware.git
cp -rf linux-firmware/* ~/arm-stuff/images/root/lib/firmware/
rm -rf linux-firmware
```

```
echo "console=tty1 debug verbose root=/dev/mmcblk1p3 rootwait rw rootfstype=ext4" > /tmp/
echo "console=tty1 debug verbose root=/dev/sda3 rootwait rw rootfstype=ext4" > /tmp/confi

vbutil_kernel --pack /tmp/newkern-sd --keyblock /usr/share/vboot/devkeys/kernel.keyblock
vbutil_kernel --pack /tmp/newkern-usb --keyblock /usr/share/vboot/devkeys/kernel.keyblock
```

06. 准备引导分区

```
dd if=/tmp/newkern-sd of=$bootp1 # first boot partition for SD
dd if=/tmp/newkern-usb of=$bootp2 # second boot partition for USB

umount $rootp

kpartx -dv $loopdevice
losetup -d $loopdevice
```

07. 用dd克隆镜像然后标记USB为可引导

```
dd if=kali-custom-chrome.img of=/dev/sdb bs=512k
cgpt repair /dev/sdb
```

这里,你要给分区1还是分区2标记更高的优先权.数字大则有更高的优先权.如下的例子将把第一个分区(用-i参数)的优先权设置成10,因为我们要从SD卡引导.

```
cgpt add -i 1 -S 1 -T 5 -P 10 -l KERN-A /dev/sdb
cgpt add -i 2 -S 1 -T 5 -P 5 -l KERN-B  /dev/sdb
```

使用**cgpt show**命令查看分区的列表和引导顺序.

```
root@kali:~# cgpt show /dev/sdb
       start        size    part  contents
           0           1          PMBR
           1           1          Pri GPT header
           2          32          Pri GPT table
        8192       32768       1  Label: "KERN-A"
                                  Type: ChromeOS kernel
                                  UUID: 63AD6EC9-AD94-4B42-80E4-798BBE6BE46C
                                  Attr: priority=10 tries=5 successful=1
       40960       32768       2  Label: "KERN-B"
                                  Type: ChromeOS kernel
                                  UUID: 37CE46C9-0A7A-4994-80FC-9C0FFCB4FDC1
                                  Attr: priority=5 tries=5 successful=1
       73728     3832490       3  Label: "Linux filesystem"
                                  Type: 0FC63DAF-8483-4772-8E79-3D69D8477DE4
                                  UUID: E9E67EE1-C02E-481C-BA3F-18E721515DBB
   125045391          32          Sec GPT table
   125045423           1          Sec GPT header
root@kali:~#
```

这个操作完成后,插入SD卡/U盘启动Chromebook(不要插在蓝色的USB口!).在开发者引导提示里按CTRL + ALT + U引导进入到Kali Linux.用(root / toor)登录到Kali,然后运行startx.

封装定制的Kali Live ISO

打造专属的Kali ISO – 简介

封装定制的Kali ISO很简单,很有趣,很有意义.你可以用Debian的live-build脚本对Kali ISO进行全面的配置.这些脚本以一系列配置文件的方式对镜像进行全面的自动定制,让任何人都可以轻易地就能打造一个Live系统镜像.官方发布的Kali ISO也采用了这些脚本.

前提

最理想的是在预装Kali的环境里定制你的Kali ISO.如果不是这样,请务必使用最新版本的live-build脚本(3.x分支的脚本可用于Debian wheezy).

准备开始

首先我们要用以下命令搭建好定制Kali ISO的环境:

```
apt-get install git live-build cdebootstrap kali-archive-keyring
git clone git://git.kali.org/live-build-config.git
cd live-build-config
lb config
```

封装Kali ISO的配置(可选)

config目录里包含了定制ISO的各种重要的自定义选项,这些选项在Debian的live build 3.x页面有文档说明.然而如果你没有耐心,请特别注意以下的配置文件:

config/package-lists/kali.list.chroot – 包含要安装在Kali ISO里的软件包的列表.你可以指定移除已经安装的软件包.也可以切换你的Kali ISO的桌面环境(KDE,Gnome,XFCE,LXDE等).

hooks/ – hooks 目录允许我们在不同阶段调用脚本封装定制Kali Live ISO.更多关于hooks的信息,参考live build 手册.举个例子,Kali是这样添加取证模式的引导菜单的:

```
$ cat config/hooks/forensic-menu.binary
#!/bin/sh

cat >>binary/isolinux/live.cfg <<END

label live-forensic
    menu label ^Live (forensic mode)
    linux /live/vmlinuz
    initrd /live/initrd.img
    append boot=live noconfig username=root hostname=kali noswap noautomount
END
```

封装ISO

在封装ISO之前,可以指定需要的架构,选择amd64或者i386.还要注意"lb build"需要root权限.如果你不指定架构,live build将根据你现在使用的架构来封装ISO.

如果你想在在32位系统封装64位的ISO,务必打开多架构支持:

```
dpkg --add-architecture amd64
apt-get update
```

配置live-build封装64位或者32位ISO:

```
lb config --architecture amd64 # for 64 bit
# ...or...
lb config --architecture i386  # for 32 bit

lb build
```

最后一个命令需要一些时间,因为它下载所有需要的软件包然后封装ISO.可以先去喝杯咖啡.

为今后封装ISO提速

如果你打算经常定制ISO,你可以把kali的软件包缓存在本地便于今后的封装.最简单的就是安装**apt-cacher-ng**,然后在每次打包时配置http_proxy环境变量.

```
apt-get install apt-cacher-ng
/etc/init.d/apt-cacher-ng start
export http_proxy=http://localhost:3142/
.... # setup and configure your live build
lb config --apt-http-proxy http://127.0.0.1:3142/
lb build
```

定制Kali的桌面系统

更换Kali的桌面环境

不是所有的Kali Linux用户都希望使用Gnome作为默认的桌面环境,所以我们简化了更换桌面管理器所需的工作.要封装一个定制过桌面环境的专属Kali ISO镜像,从封装定制的Kali Live ISO这篇文档开始吧.在封装你的ISO之前,先编辑**config/package-lists/kali.list.chroot**的最后部分,加入你选择的桌面环境的相关信息到这些注释的后面:

```
# Graphical desktops depending on the architecture
#
# You can replace all the remaining lines with a list of the
# packages required to install your preferred graphical desktop
# or you can just comment everything except the packages of your
# preferred desktop.
```

KDE

```
kali-defaults
kali-root-login
desktop-base
kde-plasma-desktop
```

Gnome

```
gnome-core
kali-defaults
kali-root-login
desktop-base
```

LXDE

```
kali-defaults
kali-root-login
desktop-base
lxde
```

XFCE

```
kali-defaults
kali-root-login
desktop-base
xfce4
```

I3WM

```
# cheers to 0xerror
xorg
dmenu
conky
i3
```

MATE

“MATE”桌面默认并没有被包含在我们的源里,集成到Kali里需要一些操作.

```
echo "deb http://repo.mate-desktop.org/debian wheezy main" >> /etc/apt/sources.list
apt-get update
apt-get install mate-archive-keyring
```

```
# apt-get install git live-build cdebootstrap
# git clone git://git.kali.org/live-build-config.git
cd live-build-config
mkdir config/archives
echo "deb http://repo.mate-desktop.org/debian wheezy main" > config/archives/mate.list.bi
echo "deb http://repo.mate-desktop.org/debian wheezy main" > config/archives/mate.list.ch
cp /usr/share/keyrings/mate-archive-keyring.gpg  config/archives/mate.key.binary
cp /usr/share/keyrings/mate-archive-keyring.gpg  config/archives/mate.key.chroot
echo "sleep 20" >> config/hooks/z_sleep.chroot
```

添加mate桌面到软件包的列表: 编辑后的config/package-lists/kali.list.chroot应该是这样:

```
xorg
mate-archive-keyring
mate-core
mate-desktop-environment
```

重新编译Kali Linux内核

有时你可能想添加必要的驱动、补丁、Kali Linux内核里没有的功能.如下的教程描述如何根据你的需要快速地修改和编译Kali Linux内核.请注意目前默认的Kali Linux内核已经打过了大量的无线注入补丁.

安装编译所需的依赖

开始安装编译内核所需的所有依赖.

```
apt-get install kernel-package ncurses-dev fakeroot bzip2
```

下载Kali Linux内核源代码

下载并解压Kali Linux的内核源代码.

```
apt-get install linux-source
cd /usr/src/
tar jxpf linux-source-3.7.tar.bz2
cd linux-source-3.7/
```

配置内核

复制Kali默认的内核配置文件然后根据你的需要修改.这一步你需要应用各种驱动、补丁、等等…在此例中,我们重新编译一个64位内核.

```
cp /boot/config-3.7-trunk-amd64 .config
make menuconfig
```

编译内核

编译你修改过的内核.需要花的时间和硬件配置有关.

```
CONCURRENCY_LEVEL=$(cat /proc/cpuinfo|grep processor|wc -l)
make-kpkg clean
fakeroot make-kpkg kernel_image
```

安装内核

内核编译成功后.继续以安装新内核,然后重启.请注意内核版本号可能不同.在此例中,当前的内核版本是3.7.2,你需要根据情况做相应的修改.

```
dpkg -i ../linux-image-3.7.2_3.7.2-10.00.Custom_amd64.deb
update-initramfs -c -k 3.7.2
update-grub2
reboot
```

重启后,你的新内核应该运行了.如果出错了导致你的内核不能启动,你仍然可以通过启动官方的Kali Linux内核来解决问题.

从源代码编译包

有时,我们需要从源代码重新编译一个Kali包.幸运的是用APT下载源代码包,进行必要的修改后再用Debian工具重新编译是如此的简单.此例中,为了添加额外的Mifare Key硬编码到mifare格式化工具，我们将重新编译libfreefare这个包.

下载包的源代码

```
# Get the source package
apt-get source libfreefare
cd libfreefare-0.3.4~svn1469/
```

修改包的源代码

按需修改包里面的源代码文件,此例中,我们以修改mifare-classic-format.c为例.

```
nano examples/mifare-classic-format.c
```

检查编译所需的依赖

检查编译包所需的依赖.它们需要在编译包前被安装.

```
dpkg-checkbuilddeps
```

输出的结果和如下类似,在于你已经安装了什么包.如果dpkg-checkbuilddeps没有任何输出,说明你没有缺少依赖,可以继续编译.

```
dpkg-checkbuilddeps: Unmet build dependencies: dh-autoreconf libnfc-dev
```

安装编译所需的依赖

安装上面**dpkg-checkbuilddeps**输出的编译所需的依赖:

```
apt-get install dh-autoreconf libnfc-dev
```

编译修改过的包

所有安装依赖安装好后,调用dpkg-buildpackage来编译是件很容易的事.

```
dpkg-buildpackage
```

安装新编译的包

如果一切顺利,你就可以安装新编译的包了.

```
dpkg -i ../libfreefare*.deb
```

ARM交叉编译

本文档说明如何在kali linux上配置ARM交叉编译环境,是我们多份关于"定制ARM镜像"的文档的起点.

开发机的配置

编译内核生成镜象通常需要大量硬盘空间.确保你的开发机至少有50G可用硬盘空间以及足够的内存,CPU不要太差.

安装依赖

先安装ARM交叉编译所需的依赖.

```
apt-get install git-core gnupg flex bison gperf libesd0-dev build-essential
zip curl libncurses5-dev zlib1g-dev libncurses5-dev gcc-multilib g++-multilib
```

如果你是64位的Kali Linux系统,用如下命令添加i386架构支持到你的开发环境.

```
dpkg --add-architecture i386
apt-get update
apt-get install ia32-libs
```

下载Linaro工具链

从我们的Git源下载Linaro交叉编译器.

```
cd ~
mkdir -p arm-stuff/kernel/toolchains
cd arm-stuff/kernel/toolchains
git clone git://github.com/offensive-security/arm-eabi-linaro-4.6.2.git
```

设置环境变量

为了能使用Linaro交叉编译器,你需要在你的session里设置如下的环境变量.

```
export ARCH=arm
export CROSS_COMPILE=~/arm-stuff/kernel/toolchains/arm-eabi-linaro-4.6.2/bin/arm-eabi-
```

现在你的ARM交叉编译环境完成了,可以编译属于你自己的ARM内核了.

准备Kali Linux ARM chroot

虽然你能从下载区下载Kali ARM镜象但是有人更热衷于定制他们的Kali rootfs.如下展示一个制作Kali armhf rootfs的例子.

安装需要的软件和依赖

```
apt-get install debootstrap qemu-user-static
```

定义架构和定制包

这里定义一些你需要的ARM架构(armel或armhf)的环境变量,下列的包将会安装到你的镜象里.这是全文要用到的,所以务必根据你的需要修改它们.

```
export packages="xfce4 kali-menu kali-defaults nmap openssh-server"
export architecture="armhf"
#export disk="/dev/sdc"
```

建立Kali rootfs

我们创建一个标准的目录结构并从Kali Linux的源用bootstrap获得ARM rootfs.然后我们从我们的主机复制**qemu-arm-static**到rootfs，以便进行第2步.

```
cd ~
mkdir -p arm-stuff
cd arm-stuff/
mkdir -p kernel
mkdir -p rootfs cd rootfs
debootstrap --foreign --arch $architecture kali kali-$architecture http://repo.kali.org/k
cp /usr/bin/qemu-arm-static kali-$architecture/usr/bin/
LANG=C chroot kali-$architecture
/debootstrap/debootstrap --second-stage
```

第2步chroot

这里我们配置基本的镜象设置，例如keymaps,源，默认网络接口特性(有需要的话请修改)等..

```
cat << EOF >    kali-$architecture/debconf.set
console-common  console-data/keymap/policy      select  Select keymap from full list
console-common  console-data/keymap/full        select  en-latin1-nodeadkeys
EOF

cat << EOF >    kali-$architecture/etc/apt/sources.list
deb http://repo.kali.org/kali kali main contrib non-free
deb http://repo.kali.org/security kali/updates main contrib non-free
EOF

echo "kali" >   kali-$architecture/etc/hostname

cat << EOF >    kali-$architecture/etc/network/interfaces
auto lo
iface lo inet loopback
auto usbmon0
iface usbmon0 inet dhcp
EOF
```

第3步chroot

这里开始定制.$Packages变量表示这个包将会被安装，默认root的密码将被设置为”toor”,以及修改和修复其它配置.

```
 mount -t proc proc kali-$architecture/proc mount -o bind /dev/ kali-$architecture/dev/ m
cat << EOF >    kali-$architecture/third-stage
#!/bin/bash debconf-set-selections /debconf.set
rm -f /debconf.set
apt-get update
apt-get -y install git-core binutils ca-certificates
apt-get -y install locales console-common less nano git
echo "root:toor" | chpasswd
sed -i -e 's/KERNEL!="eth*|/KERNEL!="/' /lib/udev/rules.d/75-persistent-net-generator.rul
rm -f /etc/udev/rules.d/70-persistent-net.rules
apt-get --yes --force-yes install $packages
rm -f /third-stage
EOF

chmod +x kali-$architecture/third-stage
LANG=C chroot kali-$architecture /third-stage
```

在chroot环境中手动配置

如果有需要,你可以手工在rootfs环境里进行最终和必要的修改.

```
LANG=C chroot kali-$architecture
{在chroot环境里做额外的修改}
exit
```

清理chroot环境里的被锁文件

事实上在rootfs里一些你已经安装的包可能会产生被锁文件(例如在chroot环境里运行中的服务),需要在我们能关闭chroot时释放.在你umount之前可能需要在chroot环境里停止一些服务.umount proc和dev的命令:

```
umount kali-$architecture/proc umount kali-$architecture/dev/pts umount kali-$architectu
```

然而,如果仍然有服务在chroot里运行,将会出现这样的错误提示:

```
root@rootfs-box:~ umount kali-$architecture/proc
root@rootfs-box:~ umount kali-$architecture/dev/pts
root@rootfs-box:~ umount kali-$architecture/dev/
umount: kali-armhf/dev: device is busy. (In some cases useful info about processes that u
```

如果出现这种情况,请用如下命令检查哪个文件/服务锁住了chroot:

```
root@rootfs-box:~/arm-stuff/rootfs:~ lsof |grep kali-armhf
...
dbus-daem 4419 messagebus mem REG 8,1 236108 15734602 dbus-daemon
dbus-daem 4419 messagebus mem REG 8,1 93472 17705250 ld-2.13.so ...
dbus-daem 4419 messagebus mem REG 8,1 100447 17705251 libpthread-2.13.so
dbus-daem 4419 messagebus mem REG 8,1 22540 17705240 librt-2.13.so
dbus-daem 4419 messagebus mem REG 8,1 893044 17705232 libc-2.13.so ...
```

从输出信息我们看到dbus守护进程仍在chroot环境里运行.在继续之前,我们需要在chroot环境里停止它.如果你已经成功umount了proc或dev,请用之前给出的命令重新挂载他们,chroot到rootfs里,然后停止dbus服务(或别的可能需要停止的服务):

```
# mount -t proc proc kali-$architecture/proc
# mount -o bind /dev/ kali-$architecture/dev/pts
LANG=C chroot kali-$architecture /etc/init.d/dbus stop exit
```

一旦释放了所有的服务和被锁文件,你就可以umount proc和dev了:

```
root@rootfs-box:~/arm-stuff/rootfs~ umount kali-$architecture/proc
root@rootfs-box:~/arm-stuff/rootfs~ umount kali-$architecture/dev/pts
root@rootfs-box:~/arm-stuff/rootfs~ umount kali-$architecture/dev/
root@rootfs-box:~/arm-stuff/rootfs~
```

清理

最后我们运行在chroot里的清理脚本释放缓存文件占用的空间,还有需要的清理工作:

```
cat << EOF > kali-$architecture/cleanup
#!/bin/bash rm -rf /root/.bash_history
apt-get update apt-get clean
rm -f cleanup
EOF

chmod +x kali-$architecture/cleanup
LANG=C chroot kali-$architecture /cleanup
/etc/init.d/dbus stop
umount kali-$architecture/proc
umount kali-$architecture/dev/pts
umount kali-$architecture/dev/
cd ..
```

恭喜！你定制的Kali ARM rootfs就在kali-$architecture目录里.你可以为往后的工作打包这个目录,或复制到一个镜像文件.

08. Kali Linux疑难排解

09. Kali 社区支持

给Kali提交问题

简介

这篇文档指导一个报告者如何提交一份最好的问题报告,以便问题能尽快的被修复.问题报告者的目的是让Kali Linux的开发者问题重现然后发现问题.如果Kali开发者发现了问题,他们会收集更多的信息直到找到问题的根本.否则,他们会要求提供更多的信息直到他们出现提交者遇到的问题.请记住,我们的开发团队使用英文,所以最好用英文提交.

Kali Linux诞生于对社区的回报.社区促使我们的项目得以更好的保持持续发展.在你写评论时请记住,为你提供支持的开发者都是无私奉献的志愿者.

想要解决问题,请明确以下的要点:

- 你是因为想要解决问题才提交的问题,所以请提供全面的信息.
- 弄清楚你提交的是事实还是假设.
- 保持问题报告的客观性,只陈述经过适当研究后的事实.
- 不要引用Wikipeida和其它非主要资源的结果作为报告.
- 一个BUG,不要以不同的报告,不同的人,不同的硬件多次提交.
- 不要把多个问题堆在一起报告,如果可以请分别提交.
- 不要发类似“Me too!” 或 “+1”这样的评论.
- 不要抱怨修复一个漏洞为何那么久.

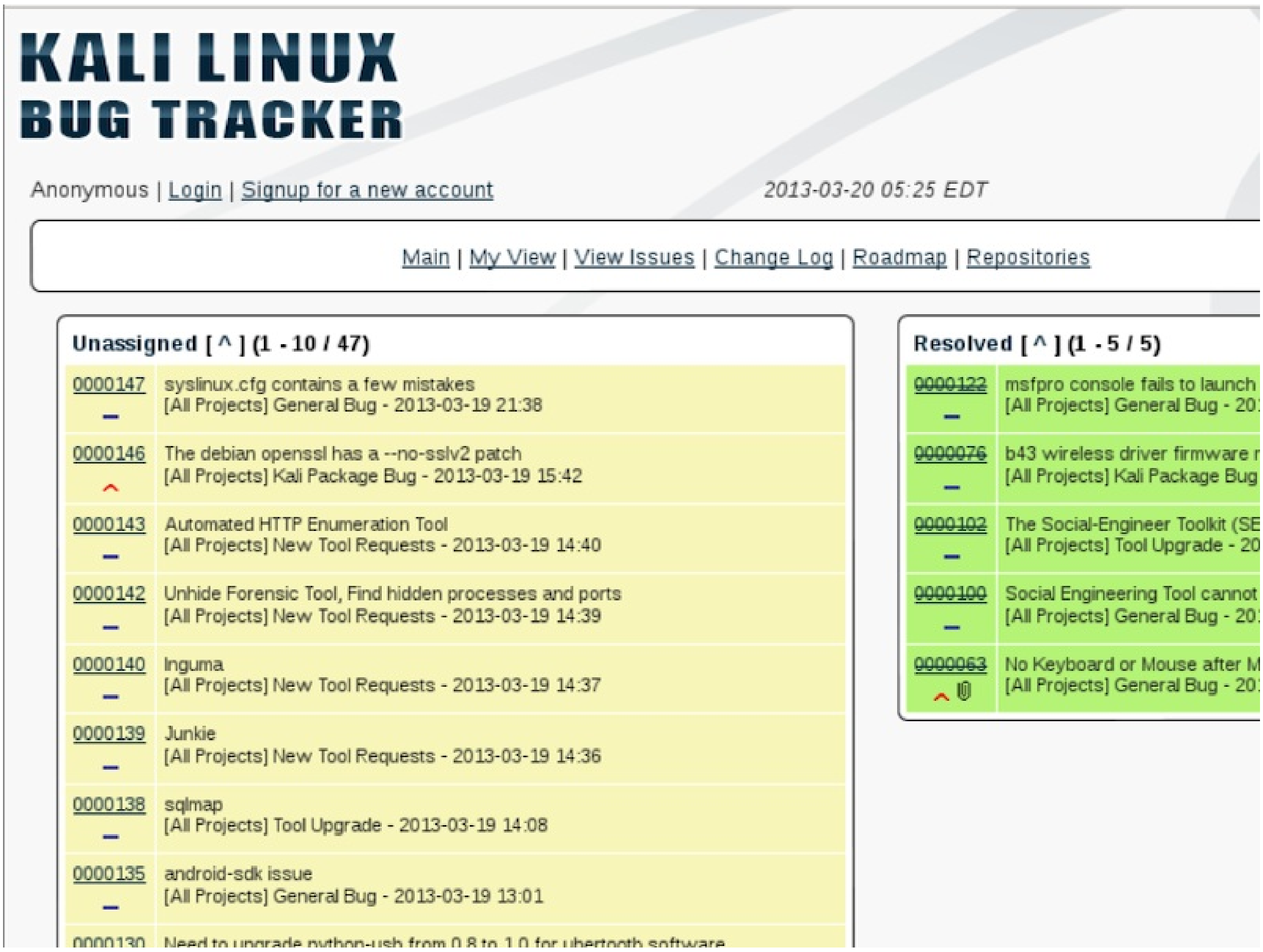
如何报告问题

Kali Linux问题追踪系统在http://bugs.kali.org.这篇文档指导你如何创建帐号,如何创建系统资料,和如何提交一份详细的报告.

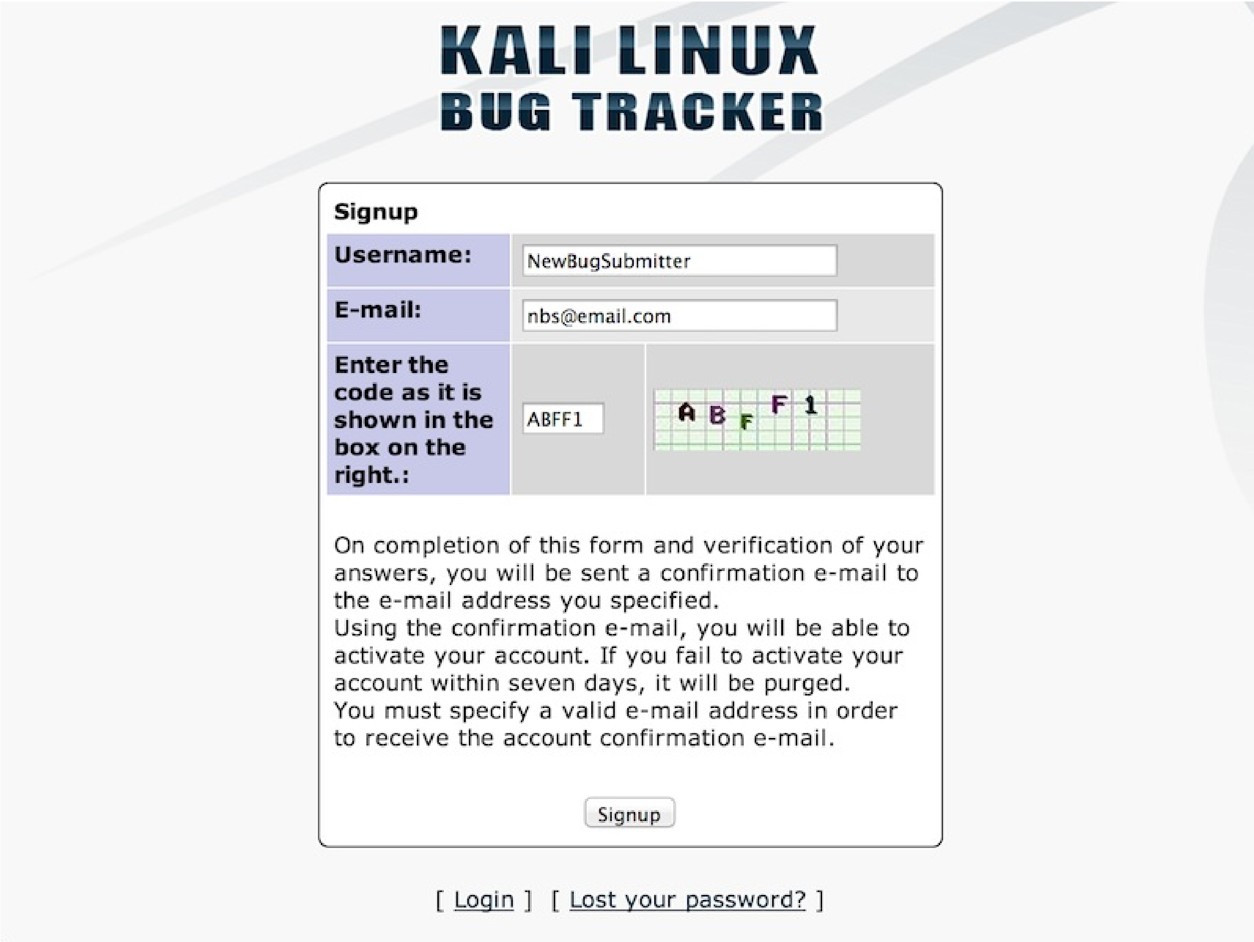
创建**Kali Linux**问题追踪系统帐户

如果你还没有创建帐户,应该先完成这一步.创建用户后你才可以提交问题报告或对已存在的问题进行评论.

在问题追踪系统页面,点击‘Signup for new account’开始创建.



输入用户名和email,然后输入验证码.点击signup按钮.



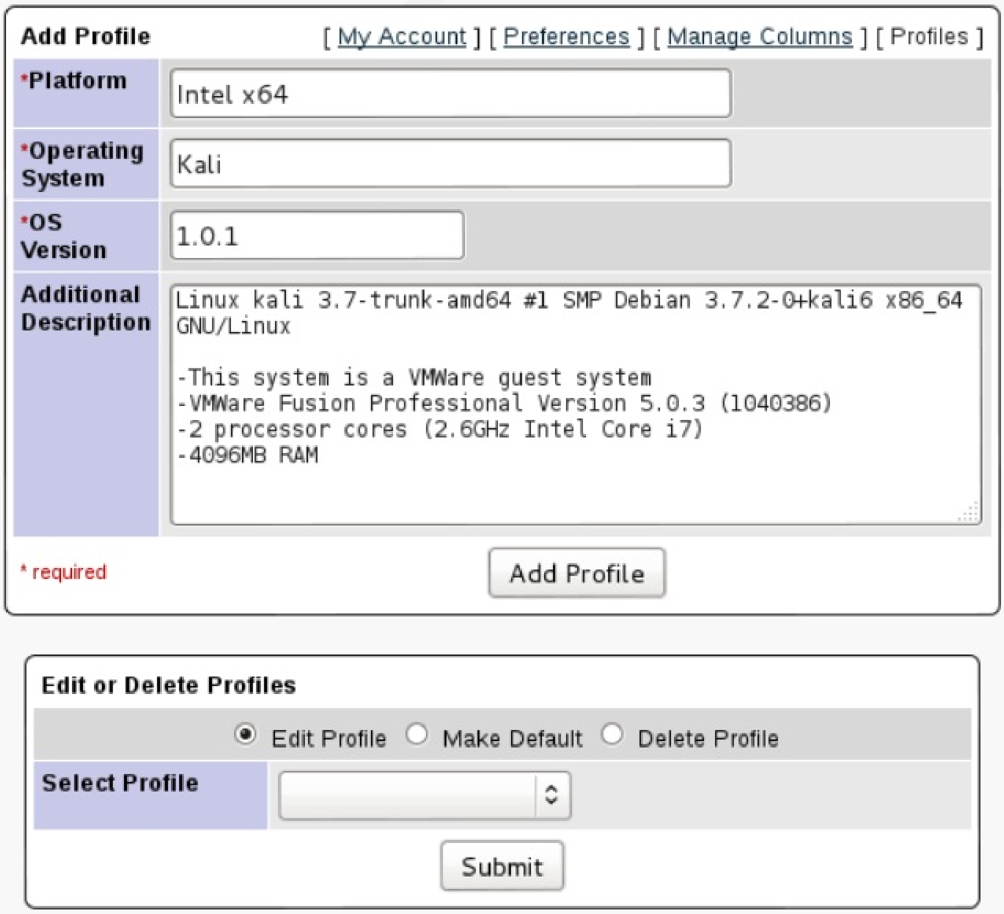
如果成功了,下一步会提示你帐户已经注册好.要激活帐户请回复官方的email确认邮件.点击"Proceed"继续到漏洞追踪系统登录页面.



在Kali Linux问题追踪系统创建一份资料

不是必须的,但是作为你的帐户的一部分,建议创建一份独特的资料.你可以为每个系统创建自定义的资料,或者从默认资料里选择.这些资料用于报告时定义你的平台,操作系统和版本信息.

创建或编辑自定义资料,从主页选择My Account然后选择Profiles.为你的系统添加具体的信息和描述,完成时点击"Add Profile"按钮.



资料添加好后,在你创建一个新的问题报告时会出现"Select Profile"下拉菜单.可以根据你的需要创建不同的配置文件,只要你在提交问题报告时选择正确的配置文件.

务必不要报告提交过的问题

在开始报告之前,在网站搜索和你的问题相关的关键字.如果存在已经被报告的问题(与硬件无关),请不要重复提交或者添加没有必要的注释,例如"Me too!"或者"+1".你可以点击ID链接来查看问题的状态.

如果你认为问题和硬件有关,即使类似的硬件也报告过,也请以你的具信息提交一份新的报告.你的硬件与别硬件不一定完全相同.不要以为同样的桌面或者笔记本型号就不可能遇到不一样的问题.

创建报告

开始你的报告,登入你的帐户然后点击登录页面上的"Report Issue".你需要填尽可能多的信息.必要时请查看本文前面提出的那几点要求.

报告中必须包含以下字段:

- Category(分类)
- Summary(摘要)

- Description(描述)

其它字段不是必须的,但我们请特别多注意下面每个选项:

- Reproducibility(重现性)
- Select Profile(选择资料)
- Steps to Reproduce(重现步骤)
- Additional Information(附加信息)
- Upload File (error logs, screenshot)-上传文件(错误日志,屏幕截图)

选择适当的分类

目前Kali的问题被分为4类.报告问题之前请先确定它的类别:

- General Bug(一般问题)
- Kali Package Bug(Kali软件包问题)
- New Tool Requests(请求添加新工具)
- Tool Upgrade(工具升级)

不要提出问题追踪系统不支持的请求.Kali Linux提供许多可选的支持,包括http://docs.kali.org , https://forums.kali.org和freenode上的IRC聊天室(#kali-linux).

提供一个描述性的摘要

摘要字段本质上是一个问题报告的"名字",Kali开发者和其它访问者会第一个看它.提供一个简短但具描述性的摘要可以描述问题或者明确要求.

Good: Chromium Package installed from Repo will not run as root user(优:从源安装的Chromium软件包不能用root运行)

Bad: Chromium doesn't work(劣:chromium不能运行)

摘要不应该包括所有东西,除非必须要包含它才能传达你提交报告的原因.

使用**dpkg**为问题报告找到软件包和软件版本

你可以用dpkg参数组合找到安装过哪个软件包.在你的报告中列入这些命令的输出结果很重要.输出结果也可以以文本文件格式上传.(在本文后面讨论).

- search
- list
- status

例子的输出:

```
root@kali:~# which chromium
/usr/bin/chromium
root@kali:~# type chromium
chromium is /usr/bin/chromium
root@kali:~# dpkg --search /usr/bin/chromium
chromium: /usr/bin/chromium
root@kali:~# dpkg --list chromium
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version      Architecture Description
+++-==============-============-============-=================================
ii  chromium       24.0.1312.68 amd64        Google open source chromium web
root@kali:~# dpkg --status chromium
Package: chromium
Status: install ok installed
Priority: optional
Section: web
Installed-Size: 98439
Maintainer: Debian Chromium Maintainers <pkg-chromium-maint@lists.alioth.debian.org>
Architecture: amd64
Source: chromium-browser
Version: 24.0.1312.68-1
…Output Truncated…
```

建立描述方案

现在是提交经过你深思熟虑的报告的时候了.尽可能多的提供细节和结果.

请务必在适当的地方包含如下内容:

- 任何错误信息的准确并完整的文本(屏幕截图或日志文件)
- 你具体输入了什么或者做过什么产生的问题
- 如果可以,提供一个修复建议或者补丁
- 软件包的版本和与依赖包有关系的任何信息
- 内核版本,C共享库,或者别看起来合适的资料
- uname –a
- dpkg -s libc6 | grep ^Version
- 适当的时候,软件版本(例如 python -V)
- 你的硬件信息
- 如果你要报告硬件驱动问题,请列出你所有的硬件信息
- 在你系统上安装源里的lshw报告完整的硬件信息
- 添加其它相关的资料
- 别为报告”太长”而担心,只要是相关信息,有比没有更好.

例子

Package: Chromium

Architecture: amd64

Maintainer: Debian Chromium Maintainers

Source: chromium-browser

Version: 24.0.1312.68-1

I installed the chromium web browser from the Kali Linux repos, using the command ‘apt-get install chromium’. I launched the program from the Kali menu by selecting Applications/Internet/Chromium Web Browser. Chromium did not launch as expected, instead it provided an error pop-up window.

The error message stated, “Chromium cannot be run as root. Please start Chromium as a normal user. To run as root, you must specify an alternate –user-data-dir for storage of profile information”.

I clicked the Close button to close the pop up window.

uname –a output: Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2+kali6 x86_64 GNU/Linux

C Library Version: 2.13-38

再现性的重要

Kali Linux问题追踪系统允许你提交被报告的问题出现频率.如果你提交一个要求添加新工具或工具更新的请求,简单的在下拉菜单选择N/A.如果提交问题,请提供相应的回答.

继续回到上面的例子,Chromium设计成无法用root启动，你可以从下拉菜单选择“总是”.

你提供了一个准确的反馈,这很重要,如果Kali开发者试图重现该问题,他们需要知道该问题的发生的频率.如果出问题的频率是偶尔,但你却标着总是,开发者可能会因为测试时没遇到问题而草率地关闭这个报告.

选择适当的资料

如上所述,为每一个报告的问题使用一个自定义的资料是最好的.如果没有创建自定义资料,从下拉菜单中选择相应的资料.在本指南发布时,下列选项是可用的.

- armel Kali 1.0
- armhf Kali 1.0
- x64 Kali 1.0
- x86 Kali 1.0

提供重现该问题的步骤

与描述部分相比这部分虽然看起来可能是多余的,但这部分只包含重现该问题采取的步骤.一些步骤可能只起辅助作用,但它们很重要务必尽力写.可能缺少的就是那个重现问题必需的步骤.

例子:

1. Opened a terminal window by selecting Applications/Accessories/Terminal
2. Typed ‘apt-get install chromium’ in the terminal and hit enter to run the command
3. Attempted to run Chromium web browser by selecting Applications/Internet/Chromium Web Browser

提供更多信息

在这部分你可以提供与问题相关的更多的信息.如果你有修复问题的方法,请在这部分提供它.同样的,坚持事实和正确的写步骤很重要,以便开发者能重现.

例子:

There is a simple fix that is well documented on several forums. I tried it and it fixed the issue for me.

- Using a text editor open /etc/chromium/default
- Add –user-data-dir flag
- i.e. CHROMIUM_FLAGS=”–user-data-dir”

Can this be patched within the repo version of Chromium so adding this flag is not required for future releases?

上传相关文件

有时提供不是很容易提供的信息给开发组很重要.报告的这部分允许你添加屏幕截图或者日志文件.注意文件的大小限制.

你可以点击”Choose FIle”按钮来添加一个文件.它会打开系统的文件管理器然后上传你选择的文件.选好文件之后点击”打开”按钮返回你的报告,然后点击”Upload File”按钮.

提交报告

至此,你已经准备好提交报告了.剩下的就是点击”Submit Report”按钮.你的报告会被提交然后分配到一个tracking ID(追踪ID).报告会在你的”My View”页面下的”Reported by Me”看见.你可以跟踪问题的解决.

摘要

问题报告的目的是帮助开发者用他们的双眼看到错误.你可以通过提供详细的说明让他们和你一起亲自看到错误.

详细描述一切,陈述采取了什么步骤,看到了什么,除了你期盼的结果外你做了什么.

尝试通过研究找到问题或解决办法.如果你可以为你的系统提供一个解决问题的方案,就可以给开发者提供同等级的问题报告.让开发者知道你到底做过什么很重要,以便让他们成功地重复过程.这不该成为你解决异常问题的绊脚石.

准确,清晰,简明扼要地写报告,以确保开发者不会误解你的意思.

开发者不会忽悠你,准备好额外的信息以便他们问起.

请对你的请求有耐心,开发者像你一样也想修复问题.我们热爱我们的工作并以继续让Kali成为有史以来最尖端的渗透测试发行版为骄傲.

这篇文章由如下的资源按需修改而成:

http://www.chiark.greenend.org.uk/~sgtatham/bugs.html – Fetched March 20,2013
https://help.ubuntu.com/community/ReportingBugs – Fetched March 20,2013
http://www.debian.org/Bugs/Reporting – Fetched March 20,2013

Kali Linux官方镜像

官方源的使用

Kali Linux提供了3类软件源,这些源在世界各地都有镜像:

- http.kali.org (镜像列表): 主要安装包软件源;
- security.kali.org (镜像列表): 安全包软件源;
- cdimage.kali.org (镜像列表): ISO镜像源.

当你使用以上的3个域名做源时,会自动连接到离你最近的与官方同步的镜像.如果你要手动选择一个镜像,请点击上面域名旁的镜像列表,选一个合适你的.

Kali Linux镜像的架设

要求

要架设一个Kali Linux的官方镜像源,你需要一台运行rsync和ssh,大硬盘 ,大带宽的服务器. 截至2013-03-14,主要安装包软件源大约160G,ISO镜像源大约10G.但应该考虑到这些数字在不停的增长. 我们希望你通过HTTP,FTP或RSYNC之一来同步镜像文件,所以必须安装相应的服务.

软件包档案的同步推送

当官方源有更新时会用基于SSH的触发器ping镜像.一般每天4次.

如果你还没有专用于镜像的帐号,先创建一个.(本例子中我们专用于镜像的专用用户是"archvsync"):

```
$ sudo adduser --disabled-password archvsync
Adding user 'archvsync' ...
[...]
Is the information correct? [Y/n]
```

创建用于存放镜像的目录,然后修改目录属主为刚才创建的专用用户:

```
$ sudo mkdir /srv/mirrors/kali{,-security,-images}
$ sudo chown archvsync:archvsync /srv/mirrors/kali{,-security,-images}
```

下一步配置rsync后台程序(按需启用后台运行)导出这些目录:

```
$ sudo sed -i -e "s/ENABLED=false/ENABLED=true/" /etc/default/rsync
$ sudo vim /etc/rsyncd.conf
$ cat /etc/rsyncd.conf
uid = nobody
gid = nogroup
max connections = 25
socket options = SO_KEEPALIVE

[kali]
  path = /srv/mirrors/kali
  comment = The Kali Archive
  read only = true

[kali-security]
  path = /srv/mirrors/kali-security
  comment = The Kali security archive
  read only = true

[kali-images]
  path = /srv/mirrors/kali-images
  comment = The Kali ISO images
  read only = true
$ sudo service rsync start
Starting rsync daemon: rsync.
```

这个文档不包括WEB服务器和FTP服务器的配置.理论上你应该导出镜像到 http://yourmirror.net/kali , http://yourmirror.net/kali-security和http://yourmirror.net/kali-images (FTP也一样). 现在是有趣的部分:专用用户处理SSH触发器配置和镜像站点的搭建.首先应该用专用用户解压ftpsync.tar.gz:

```
$ sudo su - archvsync
$ wget http://archive.kali.org/ftpsync.tar.gz
$ tar zxf ftpsync.tar.gz
```

现在我们要创建两个配置文件.在模板的基础上至少要修改*MIRRORNAME*,*TO*,*RSYNC_PATH*,和*RSYNC_HOST*这几个参数.:

```
$ cp etc/ftpsync.conf.template etc/ftpsync-kali.conf
$ cp etc/ftpsync.conf.template etc/ftpsync-kali-security.conf
$ vim etc/ftpsync-kali.conf
$ grep -E '^[^#]' etc/ftpsync-kali.conf
MIRRORNAME=`hostname -f`
TO="/srv/mirrors/kali/"
RSYNC_PATH="kali"
RSYNC_HOST=archive.kali.org
$ vim etc/ftpsync-kali-security.conf
$ grep -E '^[^#]' etc/ftpsync-kali-security.conf
MIRRORNAME=`hostname -f`
TO="/srv/mirrors/kali-security/"
RSYNC_PATH="kali-security"
RSYNC_HOST=archive.kali.org
```

最后一步建立.ssh/authorized_keys以便archive.kali.org能触发你的镜像.:

```
$ mkdir -p .ssh
$ wget -O - -q http://archive.kali.org/pushmirror.pub >>.ssh/authorized_keys
```

如果你的ftpsync.tar.gz不是解压到home目录,那么你要修正.ssh/authorized_keys中的"~/bin/ftpsync"为相应的路径. 现在发一封包含你的镜像URL的email到 devel@kali.org,以便把你的镜像加入镜像列表.请明确的指出当镜像出现问题(或要进行更改/协商镜像的配置)时我们该联系谁. 与其等待archive.kali.org的第一次推送,不如先用离你近的源进行rsync初始化同步,选择上面镜像列表里的任意一个镜像.假设你选了archive-4.kali.org,那么你应该以专用用户权限运行如下命令:

```
$ rsync -qaH archive-4.kali.org::kali /srv/mirrors/kali/ &
$ rsync -qaH archive-4.kali.org::kali-security /srv/mirrors/kali-security/ &
$ rsync -qaH archive-4.kali.org::kali-images /srv/mirrors/kali-images/ &
```

手工同步ISO镜像

ISO镜像源不使用推送同步模式,所以你要建立一个每日运行的rsync计划任务.我们提供了一个可直接用的脚本bin/mirror-kali-images,你只要配置etc/mirror-kali-images.conf,再以专用用户权限把它添加到crontab.

```
$ sudo su - archvsync
$ cp etc/mirror-kali-image.conf.sample etc/mirror-kali-images.conf
$ vim etc/mirror-kali-images.conf
$ grep -E '^[^#]' etc/mirror-kali-images.conf
TO=/srv/mirrors/kali-images/
$ crontab -e
$ crontab -l
# m h  dom mon dow   command
39 3 * * * ~/bin/mirror-kali-images
```

请设置一个精确的时间,以防archive.kali.org由于同一时间过多的同步而超负荷..

Kali Linux官方网站

Kali Linux的一系列网站用于给我们的用户提供服务.下列的是Kali官方网站以及它们的用途.请注意这些是Kali Linux发布权威信息来源的唯一的官方站点.**

下列网站是唯一的Kali Linux**发行版官方网点.**

公开的网站

- www.kali.org
- docs.kali.org
- forums.kali.org
- bugs.kali.org
- git.kali.org

Kali Linux主站主要用于发布Kali Linux相关新闻,基本信息,和一般相关项目的更新.在这里你会发现与Kali Linux相关的新工具,功能和技巧的博文.还有这应该是你下载发行版的唯一来源.

正是你现在访问的.我们的文档站点包含了一系列Kali Linux的基础文档和教程.介绍了Kali翻天覆地的变化并尝试涵盖范围广泛的常见问题.docs.kali.org这个子域名也被视为官方的(文档翻译服务器).

如果你遇到不在官方Kali Linux文档,范围的问题或情况,也许很可能有那么一位Kali Linu论坛的用户知道如何解决.你会发现Kali论坛成员来自世界各地,技术水平全面,他们热情并乐意帮助想学习的新人.

尽管我们已经为使Kali Linux完美倾尽全力,但无法预知的漏洞和错误是不可避免的.我们的改进有成效,所以当有问题或工具请求时报告给我们.我们鼓励你在bugs.kali.org提交bug报告,帮助我们把Kali Linux做得更好.

我们的Git树,供那些想密切关注Kali Linux开发或想知道他们什么时候应该运行‘apt-get upgrade’的用户查阅.

社交媒体

- twitter
- facebook

我们在有重要信息的时候才发推.发布信息和博客文章都会被推送到我们的twitter.账户是@KaliLinux.

帐户和Twitter的一样.我们不会在我们的Kali Facebook page灌水,除了有价值的文章.

Kali Linux漏洞追踪

Kali Linux有官方的漏洞追踪系统,用户可以提交漏洞或者补丁给开发者,或者给我们的发行版提交新的工具包.任何人都能在漏洞追踪系统注册,但是我们建议你先看如下规则,以保证漏洞用正确的信息和适当的格式提交给我们.

- 漏洞追踪系统不是客服系统.
- 使用真实的email以便我们在将来需要的时候能及时联系你.
- 使用明确的标题.
- 尽可能多的提供细节,包括终端输出,系统架构类型和准确的版本.
- 提交新工具包时必须包含新增这个工具的理由和它的URL.
- 不要把BUG共享给任何人一起提交,开发者会判断是谁发现的BUG.

10. Kali Linux 策略

Kali Linux安全更新策略

Kali Linux和Debian的源有紧密的联系,因此安全更新会像Debian发行版一样频繁,更新的都是debian维护的包(大部分).其它包则由Kali团队尽力的维护.

Kali Linux网络服务策略

Kali Linux处理网络服务这点上与大部分别的发行版不同.最主要的是Kali默认不启用任何外部监听的服务,目的是在渗透测试时保持最低程度的探测.

Kali默认安装了很多服务,例如Apache和SSH.但在需要时你要手动运行他们.

Kali Linux Root用户策略

大部分发行版鼓励它们的用户使用一般用户权限来操作.这是个明智的安全忠告,它使得用户和OS之间有一个额外的保护层.特别是对于需要权限分离的多用户系统.

Kali Linux本质上是一个安全和审计平台,许多工具都需要用root权限运行.通常,使用Kali Linux时,不可能是多用户环境,因此默认用户是”root”.此外不建议Linux新手使用Kali Linux,因为他们在使用超级用户时更容易制造毁灭性的错误.

渗透测试工具策略

Kali Linux工具策略

我们知道很多的工具或脚本都能做同样的工作.有的比较好用,有的是喜好问题.为此,保持渗透测试软件源的更新和可用是一项极具挑战性的任务.Kali开发组使用如下检验标准来判断一个工具是否被包含在我们的发行版.

- 在渗透测试环境下该工具是否 可用/实用?
- 该工具的功能是否与别的工具重复?
- 该工具是否允许自由地重新分发?
- 该工具的依赖关系如何?能否在"独立"环境下运行?

根据这些问题的答案和其它的因素,才决定该工具是否要标记包含在Kali.

多数Kali开发组成员都从事渗透测试工作,结合我们的经验,同时从其它方面考虑,从而为Kali发行版选择最有价值,最好的工具.以DOS,DDOS为目的或无名的工具很少用于合法用途,因此默认不会被安装在Kali Linux.

请求添加新工具

我们的大门永远向新的和更好的工具敞开,但是每个工具都必须是有效的.请在提交工具上放一些心思和精力,不要只给开发者发一行消息.可以通过我们的Kali Linux漏洞追踪系统提交新的工具请求..

Kali Linux开源软件策略

Kali Linux的 `主要` 包含了数以千计的自由软件包.作为Debian的衍生版,Kali所有的自由软件都遵循Debian的自由软件准则.

与上述不同的是,Kali Linux的 `非自由软件` 部分包含了一系列由Offensive Security重新分发的非开源工具,这些工具已经经过开发商的默认许可或特别许可.在把每个Kali专有的非开源软件包导入到你的Kali衍生版之前,你应该先详查这个软件包的授权(从Debian导入的非开源软件包除外).

更重要的是,所有Kali的专有开发或软件整合都已经投入到GNU GPL下.

如果你想获得更多关于指定软件授权的信息,可以查阅源码包中的 `debian/copyright` 或从 `/usr/share/doc/_package_/copyright` 查阅已经安装的包的授权信息.

Kali Linux商标策略

Kali Linux和Offensive Security希望我们的商标在网络社区获得广泛的认同,但是也要确保我们的商标用于我们的公司和产品.我们的商标核心策略是信任-避免用户在与Kali Linux和/或Offensive Security交涉的问题上产生误会.这影响到渗透测试发行版的开发和分发(例如Kali Linux)的可信度.

这份文档展示和描述我们的商标,并提供合理使用它们的指南.我们很乐意你公平和诚实地使用我们的商标.如果有意向的话,详细咨询请随时与我们联系.

我们的一些商标

用于打印,网页,媒体和公开展示

保持商标的外形和拼写很重要.请勿修改商标.包括使用缩写名、添加LOGO、与其它词汇合并.我们建议你像我们一样正确的使用商标.

Offensive Security商标表示源自我们的产品和服务.我们希望商标只用于辨认Offensive Security的产品和服务.以避免用户在与我们交涉的问题上产生误会.

首先提到Offensive Security的商标应该伴随标志符号,已注册的商标用"?",未注册的商标用"?".如果有疑虑,请参考上面列表使用"?"的正确符号.

使用Offensive Security商标应该与周围的大写、斜体、粗体或带下划线的文本分开.Offensive Security商标表示其源自我们的产品和服务.

在书面材料使用Offensive Security商标时,应该提供一个[此商标]是Offensive Security商标的声明.例如:

"KALI LINUX ?是Offensive Security的商标."这个声明可以适当的放在你的文本,或脚注或者尾注里.

禁止将Offensive Security商标用于你的域名,因为这样使用将导致客户误会.在商标策略范围以外的,不得未经Offensive Security明确的书面许可使用.

可以用于印制T恤,做电脑桌面,或制作别的有Offensive Security商标的制品,仅限本人和朋友(未能从中获利).在没有获得书面许可时,不得把商标用于商业生产(无论是否盈利).

联系

如果你有任何问题或者评论,或者想举报滥用Offensive Security商标,请联系我们.

Kali和Debian的关系

Kali Linux 1.0基于Debian Wheezy.因此,大部分的Kali包都是从Debian源原封不动的导入.还有些比较新的包因为可以提升用户体验或存在必须修复的BUGS,所以从不稳定版或者实验版导入.

分离包

为了实现一些Kali特有的功能,一些包明显的必须被分离.但Kali在可能时尽量靠提高上游包的数量来保持分离包的数量最小化(直接整合功能,或添加所需的钩子而不用修改上游包).

每个被Kali分离的包以Debian的Git 源分支的方式维护,简单把*Git* 源和Debian主分支合并,以便升级一个被分离的包变得很容易.

新包

此文前面提到,Kali引入了很多新的用于渗透测试和安全审计领域的Debian包.依据Debian的自由软件准则,这些大部分都是自由软件.Kali打算把它们贡献给Debian并且直接在Debian里维护它们.

因此,Kali包努力遵循Debian 策略并且在Debian里表现良好.